Tecnología de la Información. La Norma IRAM-ISO/IEC 17799 sobre el Código de Práctica para la Gestión de la Seguridad de la Información.[1]

Armando M. Casal

Resumen

Considerando las amenazas, cada vez más sofisticadas y en aumento, a las cuales está expuesta la información de las organizaciones, surge la necesidad de definir pautas para resguardarla. El artículo analiza la norma técnica IRAM-ISO/IEC 17799 (que fue renumerada como 27002) sobre tecnología de la información -Código de Práctica para la Gestión de la Seguridad de la Información-, poco conocida por la profesión contable. Esta representa un estándar reconocido internacionalmente, considerando que las empresas de todo tamaño o naturaleza tienen, en menor o mayor medida, un cierto nivel de dependencia informática, lo que implica que sean más vulnerables a los retos de seguridad.

Palabras Clave: Buenas Prácticas Corporativas; Seguridad Informática; Sistemas de Gestión de Seguridad; Seguridad de la Información; Políticas de Seguridad.

Abstract

It is necessary to provide guidance for protecting information in corpora-

1 Esta Colaboración forma parte del libro "GOBIERNO CORPORATIVO. DIRECCIÓN, ADMINISTRACION Y CONTROL DE ORGANIZACIONES EN FORMA ÉTICA Y RESPONSABLE", cuyo autor es el Dr. Armando Miguel Casal, Errepar, noviembre 2010, prologado por el prestigioso Profesor Jorge Tua Pereda y el Dr. Sergio Villagarcia, managing partner para Latinoamérica de PKF Internacional. Se agradece a Sergio Omar Garcia y a Enzo Taibi por sus valiosos y oportunos comentarios y aportes. Todo error y/u omisión subyacente es de exclusiva responsabilidad de los autores.

tions which may be harmed by even more sophisticated threats on the increase. This article analyzes the technical standard IRAM-ISO/IEC 17799 (renumbered as 27002) about Information Technology -Code of Practice for Information Security Management-, barely known by the accounting practice. It is an internationally accepted worldwide standard and, considering that all companies, no matter their size or their nature, depend to a greater or lesser extent, on information technology, they are more vulnerable to security risks.

Key Words: Good Corporate Practices, Information Technology Security, Information Security Management System, Information Security, Security Policies.

Clasificación JEL: M1, M4.

1. Introducción

El dictado de buenas prácticas corporativas voluntarias en distintos sectores de la economía de nuestro país y/u obligatorias conforme a las normas legales y reglamentarias que correspondan están también apuntaladas por la norma IRAM-ISO/IEC 17799/2002 referente al manejo de la seguridad de la información. Es un modelo reconocido internacionalmente que es utilizado en todo tipo de organizaciones y aplicaciones. No es relevante el tamaño de la empresa, ya que lo importante es el "grado de dependencia informática".(1)

Ese estándar de seguridad informática se refiere a la Tecnología de la Información dando un "Código de Práctica para la Gestión de la Seguridad de la Información". Representa un marco común para todo requerimiento de auditoría interna, auditoría externa, o proveniente de clientes, proveedores o socios estratégicos.(2)

Definición de norma:

"Un documento establecido por consenso y aprobado por un organismo reconocido que establece, para usos comunes y repetidos, reglas, criterios o características para las actividades o sus resultados, que procura la obtención de un nivel óptimo de ordenamiento en un contexto determinado" (norma IRAM 50-1:1992, basada en la Guía ISO/IEC 2:1991).

Un *estándar* representa un comprobante público y, en consecuencia, puede ser consultado, referenciado y usado por quienes lo deseen, siendo su aplicación voluntaria aunque, en algunos casos, las autoridades gubernamentales pueden dictar reglamentos obligatorios que hacen referencia a *normas* para mejorar la calidad, la seguridad y la competitividad empresarial. Están en constante revisión y este proceso se reinicia cada vez que se formulen observaciones fundamentadas, o cuando el estándar/norma se torna obsoleto debido a los avances científico-tecnológicos en el tema.

El Instituto Argentino de Normalización (IRAM), representante de la Argentina en la ISO (*International Organization for Standarization*), constituye una asociación que establece normas técnicas, estimula el conocimiento y la aplicación de la normalización, y promueve las actividades de certificación de productos y de sistemas de la calidad en las empresas, en el marco del decreto 1474/1994. Fue creado en el año 1935 y en febrero de 1995 fue reconocido como el Organismo Nacional de Normalización de la República Argentina.

La norma IRAM-ISO/IEC 17799 constituye una adopción idéntica de la norma ISO/IEC 17799/2000 (solamente el IRAM ha agregado el Anexo A, "Glosario de términos"). A su vez, la norma ISO se basa en el estándar internacional BS (*British Standard*) 7799 - Parte 1. la cual proporciona un modelo de buenas prácticas en la gestión de la información. Este arquetipo puede ser empleado por las empresas para implementar un Sistema de Gestión de Seguridad en la Información. *The International Organization for Standardization* (ISO), creada en el año 1947, y *The International Electrotechnical Commission* (IEC), componen el sistema especializado de estandarización en todos los lugares del mundo.(3)

Actualmente, la norma argentina IRAM-ISO/IEC 27002, "Tecnología de la información. Técnicas de seguridad. Código de práctica para la gestión de la seguridad de la información", cuya primera edición data del 15 de agosto de 2008, forma parte de la Serie 27000, habiendo surgido varios cambios de redacción y en la distribución de los conceptos.

El Sistema de Gestión de Seguridad en la Información puede ser certificado por un organismo externo acreditado. En este caso, el estándar internacional a aplicar es la BS 7799 - Parte 2. que garantiza que la información que se maneja (especificaciones, fórmulas, información de nuevos lanzamiento de pro-

ductos, datos claves del mercado, etc.) se administra dentro de un marco de confidencialidad y seguridad.

La seguridad de la información se define como la preservación de las siguientes características:

a) confidencialidad: se garantiza que la información sea accesible sólo a aquellas personas autorizadas a tener acceso a ella.

b) integridad: se salvaguarda la exactitud y totalidad de la información y los métodos de procesamiento.

c) disponibilidad: se garantiza que los usuarios autorizados tengan acceso a la información y a los recursos relacionados con ella, toda vez que se requiera.

Necesidad de la seguridad de la información

La información y los procesos, sistemas y redes que le brindan apoyo constituyen importantes recursos de la empresa. La confidencialidad, integridad y disponibilidad de la información pueden ser esenciales para mantener la ventaja competitiva, el flujo de fondos, la rentabilidad, el cumplimiento de las leyes y la imagen comercial.

Las organizaciones y sus redes y sistemas de información se enfrentan en forma creciente con amenazas relativas a la seguridad de diversos orígenes, incluyendo el fraude asistido por computadora, espionaje, sabotaje, vandalismo, incendio o inundación. Daños tales como los ataques mediante virus informáticos, *hacking* y denegación de servicio se han vuelto comunes, ambiciosos y crecientemente sofisticados.

La dependencia de las organizaciones respecto de los sistemas y servicios de información denota que ellas son más vulnerables a las amenazas concernientes a la seguridad.

Muchos sistemas de información no han sido diseñados para ser seguros.

Recursos para el establecimiento de los requisitos de seguridad

- Evaluar los riesgos que enfrenta la organización, identificando las amenazas a los activos, evaluando las vulnerabilidades y probabilidades de ocurrencia, y estimando el impacto potencial.
- Requisitos legales, normativos, reglamentarios y contractuales que deben

cumplir la organización, sus socios comerciales, los contratistas y los prestadores de servicios.
- Conjunto específico de principios, objetivos y requisitos para el procesamiento de la información, que ha desarrollado la organización para respaldar sus operaciones.

Requisitos básicos para implementar un sistema de gestión de seguridad en la información
- Establecer una política de seguridad en la información.
- Realizar un análisis de los riesgos en la administración de la información.
- Implementar los controles para hacer frente a tales riesgos, conforme a los requisitos de la norma.
- Evaluar la eficacia de los controles establecidos.
- Mejorar el sistema en forma continua (concepto de calidad total).

Beneficios para una organización que base su política de seguridad en tales normas
- Aumento de los niveles de seguridad, por una gestión eficaz de sus recursos de información críticos y los mecanismos de protección adecuados, lo que redundará en una reducción efectiva de los niveles de riesgos y vulnerabilidades, que se traduce en ahorro de tiempo, dinero y en un fortalecimiento de la imagen institucional.
- Planificación de las actividades, por medio de las áreas relevantes de controles con el propósito de hacer más seguros sus sistemas y cumplir con los objetivos del ente.
- Mejora continua, puesto que se consideran los criterios de revisión y mejora permanente a ser empleados para mantener los niveles de seguridad.
- Posicionamiento estratégico, permitiendo a las organizaciones enfrentar desafíos, ampliar sus actividades y competencias, teniendo impacto en las perspectivas de crecimiento, en la eficiencia operativa y en la calidad del servicio/producto brindado.
- Cumplimiento de normas y reglamentaciones, posibilitando alinear los esfuerzos y recursos de la entidad de común acuerdo con lo dispuesto por las normativas que la alcance.

- Posicionamiento en un esquema comparativo con otras organizaciones, permitiendo crear un marco homogéneo para comparar el posicionamiento frente a la seguridad de la información.

Puntos a considerar para la evaluación metódica de los riesgos en materia de seguridad

- Impacto potencial de una falla de seguridad en los negocios, teniendo en cuenta las potenciales consecuencias por una pérdida de la confidencialidad, integridad o disponibilidad de la información y otros recursos.
- Probabilidad de ocurrencia de dicha falla tomando en cuenta las amenazas y vulnerabilidades predominanes, y los controles actualmente implementados.

Controles que se consideran esenciales para una organización desde el punto de vista legal

- Protección de datos y confidencialidad de la información personal.
- Protección de registros y documentos de la organización.
- Derechos de propiedad intelectual.

Controles considerados como práctica recomendada de uso frecuente en la implementación de la seguridad de la información

La seguridad de la información se logra implementando un conjunto adecuado de controles, que abarca políticas, prácticas, procedimientos, estructuras organizacionales y funciones de software. Se deben establecer estos controles para garantizar que se logren los objetivos específicos de seguridad de la organización, reduciendo los riesgos a un nivel aceptable.

Los controles deben seleccionarse teniendo en cuenta el costo de implementación en relación con los riesgos a reducir y las pérdidas que podrían producirse, de tener lugar una violación de la seguridad. También deben tenerse en cuenta los factores no monetarios, como el daño a la reputación.

- Documentación de la política de seguridad de la información.
- Asignación de responsabilidades en materia de seguridad de la información.
- Instrucción y entrenamiento en materia de seguridad de la información.

- Comunicación de incidentes relativos a la seguridad.
- Administración de la continuidad de la empresa.

Objetivos de las revisiones periódicas de los riesgos de seguridad y de los controles implementados

- Reflejar los cambios en los requerimientos y prioridades de la empresa.
- Considerar nuevas amenazas y vulnerabilidades.
- Corroborar que los controles siguen siendo eficaces y apropiados.

Factores críticos de éxito para la implementación de la seguridad de la información dentro de una organización

- Política de seguridad, objetivos y actividades que reflejen los objetivos de la empresa.
- Estrategia de implementación de seguridad que sea consecuente con la cultura organizacional.
- Apoyo y compromiso manifiesto por parte de la gerencia.
- Claro entendimiento de los requerimientos de seguridad, la evaluación de riesgos y la administración de los mismos.
- Comunicación eficaz de los temas de seguridad a todos los gerentes y empleados.
- Distribución de guías sobre políticas y normas de seguridad de la información a todos los empleados y contratistas.
- Instrucción y entrenamiento adecuados.
- Sistema integral y equilibrado de medición que se utilice para evaluar el desempeño de la gestión de la seguridad de la información para brindar sugerencias tendientes a mejorarlo.

Norma IRAM 17798 - Requisitos para los sistemas de gestión de la seguridad de la información. Su relación con la norma IRAM-ISO/IEC 17799.

La norma argentina IRAM 17798/2004 trata los "requisitos para los sistemas de gestión de la seguridad de la información" (*Requirements for information security management systems*), y tiene como propósito brindar a la dirección de las empresas y su personal un modelo de implementación y ges-

tión de la seguridad de la información (SGSI), recomendándose que su adopción sea una decisión estratégica para una organización.(4)

Los controles que se especifican en su Anexo A, "Objetivos de control y controles", se refieren a: 1. Políticas de seguridad (*Security Policy*); 2. Seguridad de la organización (*Organizational Security*); 3. Clasificación y control de activos (*Asset Classification and Control*); 4. Seguridad del personal (*Personnel Security*); 5. Seguridad física y ambiental (*Physical and Environmental Security*); 6. Gestión de comunicaciones y operaciones (*Communications and Operations Management*); 7. Control de acceso (*Access Control*); 8. Desarrollo y mantenimiento de sistemas (*Systems Development and Maintenance*); 9. Gestión de la continuidad de los negocios (*Business Continuity Management*); y 10. Cumplimiento (*Compliance*). Su diseño está influenciado por las necesidades del negocio y sus objetivos, los requisitos de seguridad establecidos, los procesos utilizados, y el tamaño y estructura de la organización, pudiendo ser empleada por partes internas y externas, incluyendo a los organismos de certificación, para evaluar la capacidad de un ente para cumplir con sus propios requisitos, las demandas de cualquier cliente o las regulaciones que lo afecten. La certificación de procesos ayuda a enfocarse en la mejora de la seguridad de la información y permite así avances en la gestión de la información.

El modelo conocido como Planificar-Hacer-Verificar-Actuar (PHVA) se puede aplicar a todos los procesos del SGSI, como se adopta en la norma IRAM 17798, la cual consta de los siguientes temas: 1. Objeto y campo de aplicación; 2. Documentos normativos para consulta; 3. Términos y definiciones; 4. Sistema de gestión de seguridad de información; 5. Responsabilidad de la dirección; 6. Revisión del SGSI por la dirección; 7. Mejora del SGSI; Anexo A, Objetivos de control y controles; Anexo B, Guía del uso de la norma. Su enfoque está basado en procesos para establecer, implementar, operar, realizar el seguimiento, mantener y mejorar la eficacia de un SGSI en una organización; siendo un "proceso", cualquier actividad que emplee recursos y esté gestionada para permitir la transformación de las entradas en salidas; y alienta a los usuarios a resaltar la importancia de los siguientes puntos: a) comprender los requisitos de seguridad de la información de la empresa y la necesidad del establecimiento de políticas y objetivos para dicha seguridad de la información; b) implementar y operar controles dentro del manejo de la gestión de los

riesgos de la organización; c) efectuar el seguimiento y la revisión del desempeño y la eficacia del SGSI; y d) implementar el proceso de mejora continua basada en mediciones objetivas.

Por su parte, la guía del Código de Prácticas de la Norma IRAM-ISO-IEC 17799, en sus capítulos o secciones 3 a 12, provee una orientación y recomendaciones para la implementación de una buena práctica para sostener los controles antes especificados. Su contenido por grandes títulos comprende: 3. Política de Seguridad (Política de seguridad de la información); 4. Organización de la seguridad (Infraestructura de seguridad de la información; Seguridad frente al acceso por parte de terceros; Tercerización); 5. Clasificación y control de activos (Responsabilidad por rendición de cuentas de activos; Clasificación de la información); 6. Seguridad del personal (Seguridad en la definición de puestos de trabajo y la asignación de recursos; Capacitación del usuario; Respuesta a incidentes y anomalías en materia de seguridad); 7. Seguridad física y ambiental (Áreas seguras; Seguridad del equipamiento; Controles generales); 8. Gestión de comunicaciones y operaciones (Procedimientos y responsabilidades operativas; Planificación y aprobación de sistemas; Protección contra el software malicioso; Mantenimiento; Administración de la red; Administración y seguridad de los medios de almacenamiento; Intercambios de información y software); 9. Control de accesos (Requerimientos del negocio; Administración de accesos de usuarios; Responsabilidades del usuario; Control de acceso a la red; Control de acceso al sistema operativo; Control de acceso a las aplicaciones; Monitoreo del acceso y uso de los sistemas; Computación móvil y trabajo remoto); 10. Desarrollo y mantenimiento de sistemas (Requerimientos de seguridad de los sistemas; Seguridad en los sistemas de aplicación; Controles criptográficos; Seguridad de los archivos del sistema; Seguridad de los procesos de desarrollo y soporte); 11. Administración de la continuidad de los negocios (Aspectos de la administración de la continuidad de los negocios); y 12. Cumplimiento (Cumplimiento de requisitos legales; Revisiones de la política de seguridad y la compatibilidad técnica; Consideraciones de auditoría de sistemas). Anexos informativos: Anexo A - Glosario; Anexo B - Bibliografía; y Anexo C - Integrantes de los organismos de estudio.

Clasificación de guías globales sobre seguridad de la información.

El Código de Prácticas podría ser entendido como un punto de partida para el desarrollo de lineamientos propios o más específicos, aplicables a cada empresa: a) no todas las guías y controles resultarán aplicables a todos los casos; y b) probablemente deberían agregarse, para casos concretos, controles no incluidos en la norma.

Detalle de guías

El alcance de la primera versión de *Information Security Harmonisation* identifica, clasifica e informa sobre las guías más comúnmente conocidas y aceptadas en el mundo, *Classification of Global Guidance*[5]:

1. Control Objectives for Information and related Technology (COBIT);
2. Systems Security Engineering;
3. Generally Accepted Information Security Principles (GAISP);
4. The Information Security Forum's (ISF's) Standard of Good Practice for Information Security;
5. ISO/IEC 13335 Information Technology-Guidelines for the Management of IT Security;
6. ISO/TR 13569:1997 Banking and Related Financial Services-Information Security Guidelines;
7. ISO/IEC 15408:1999 Security Techniques-Evaluation Criteria for IT Security;
8. BS 7799 Part 2:2002 Information Security Management Systems-Specification With Guidance for Use;
9. ISO/IEC 17799:2000 Information Technology-Code of Practice for Information Security Management;
10. The IT Infrastructure Library's (ITIL's) Security Management;
11. NIST 800-12 An Introduction to Computer Security-The NIST Handbook;
12. NIST 800-14 Generally Accepted Principles and Practices for Securing Information Technology Systems;
13. NIST 800-18 Guide for Developing Security Plans for Information Technology Systems;
14. NIST 800-53 Recommended Security Controls for Federal Information Systems;
15. Operationally Critical Threat, Asset, and Vulnerability Evaluation (OCTAVE), Criteria Versión 2.0 Networked Systems Survivability Program;

16. Organisation for Economic Cooperation and Development (OCED) Guidelines for the Security of Information Systems and Networks.

Modelo de política de seguridad en el sector público basado en la norma IRAM-ISO/IEC 17799.

En el Sector Público, la Oficina Nacional de Tecnologías de Información (ONTI), en setiembre de 2003, convocó a distintos Organismos de la Administración Pública para conocer sus opiniones sobre estrategias de seguridad, surgiendo la necesidad de que dichos Organismos contaran con una guía de seguridad escrita.

Se conformó un grupo de trabajo para redactar un Modelo de Política de Seguridad, y se acordó basarse en la norma IRAM/ISO 17799. La Jefatura de Gabinete de Ministros aprobó en diciembre 2004, la Decisión Administrativa (DA) 669/2004, comenzándose a difundir la norma y el modelo.

Su contenido implica: a) dictar o adecuar la política de seguridad de la información en la Administración Nacional y los Entes Públicos; b) conformar, en sus ámbitos, un Comité de Seguridad, y c) asignar las responsabilidades en materia de seguridad de la información, siendo sus objetivos prácticos: 1. revisar y proponer la política de seguridad de la información; 2. acordar y aprobar metodologías y procesos específicas; 3. evaluar y coordinar la implementación de controles; 4. coordinar el proceso de administración de la continuidad de la operatoria del Organismo; 5. monitorear cambios significativos en los riesgos; y 6. tomar conocimiento y supervisar la investigación de los incidentes relativos a la seguridad.

2. Desarrollo de la Norma IRAM-ISO/IEC 17799 Tecnología de la Información. Código de Práctica para la Gestión de la Seguridad de la Información (*Information Technology - Code of Practice for Information Security Management*).

La información puede existir en diversas formas y constituye un elemento valioso para las organizaciones y las amenazas a las cuales está expuesta son cada vez más sofisticadas y aumentan día a día. A fin de lograr una mayor protección de la información, surge la necesidad de definir pautas para res-

guardarla. La norma ISO/IEC 17799, confirmada en nuestro país como IRAM 17799, nació en respuesta a dicha necesidad, siendo una compilación de recomendaciones para las prácticas exitosas de seguridad que toda entidad puede aplicar en todos los ambientes.

Normalmente las organizaciones tienen un nivel alto de dependencia informática, implicando que sean más sensibles a los desafíos de seguridad, y por otra parte, los sistemas dialogan con otros sistemas, resultando lógico deducir que los parámetros de seguridad empleados se ajustan, debiendo ser compatibles entre sí.

La implementación de la norma presenta ventajas relacionadas con las auditorías internas y externas, existiendo una tendencia a su uso, aunque no exista una ley que lo imponga. Además, una empresa que esté certificada puede ganar frente a competidores no certificados, ya que el cliente potencial, para el cual la seguridad sea un aspecto importante, optará por la organización que cumpla con las características inherentes al cumplimiento del estándar.

La norma define a la información, como "un recurso, que como el resto de los importantes activos comerciales, tiene valor para una organización y por consiguiente debe ser debidamente protegida".

Considera que la seguridad de la información, que deberá preservar básicamente las características de confidencialidad, integridad y disponibilidad, que suelen ser primordiales para "mantener la ventaja competitiva, el flujo de fondos, la rentabilidad, el cumplimiento de las leyes y la imagen comercial, protege a ésta de una amplia gama de amenazas, a fin de garantizar la continuidad comercial, minimizar el daño a la misma y maximizar el retorno sobre las inversiones y las oportunidades".

Entiende que *la información puede existir en muchas formas*, como "estar impresa o escrita en papel, almacenada electrónicamente, transmitida por correo o utilizando medios electrónicos, presentada en imágenes, o expuesta en una conversación y cualquiera sea la forma que adquiere la información, o los medios por los cuales se distribuye o almacena, siempre debe ser protegida en forma adecuada".

El Código de Práctica para la Gestión de la Seguridad de la Información destaca lo siguiente:

- las organizaciones, sus redes y sistemas de información, afrontan de manera creciente amenazas, de diversos orígenes, vinculadas con la seguridad;

- la dependencia de las organizaciones respecto de los sistemas y servicios de información indica que son más vulnerables al "fraude asistido por computadora, espionaje, sabotaje, vandalismo, incendio o inundación";
- muchos sistemas de información no fueron diseñados para ser seguros, siendo limitada la seguridad que puede obtenerse por medios técnicos, debiendo respaldarse por una gestión y procedimientos apropiados;
- resulta fundamental que una empresa identifique sus requerimientos de seguridad, considerando: a) la evaluación de los riesgos que enfrenta la organización; b) la determinación de los requisitos legales, normativos, reglamentarios y contractuales que se deben cumplir; y c) la definición de los principios, objetivos y requisitos para el procesamiento de la información;
- los requerimientos de seguridad se identifican por medio de una evaluación de los riesgos de seguridad considerando: a) el impacto potencial de una falla de seguridad en los negocios, y b) la probabilidad de ocurrencia de la falla, tomando en consideración las amenazas y debilidades, así como los controles actualmente implantados;
- deben seleccionarse e implementarse los controles para garantizar que los riesgos se mitiguen o reduzcan a un nivel razonable;
- algunos controles son considerados principios rectores para proveer un punto de partida adecuado para la implementación de la seguridad de la información, a saber: "a) protección de datos y confidencialidad de la información personal; b) protección de registros y documentos de la organización; c) derechos de propiedad intelectual", siendo los controles de uso frecuente para dicha implementación: "a) documentación de la política de seguridad de la información; b) asignación de responsabilidades en materia de seguridad de la información; c) instrucción y entrenamiento en materia de seguridad de la información; d) comunicación de incidentes relativos a la seguridad; e) administración de la continuidad de la empresa";
- ciertos factores resultan críticos para la implementación exitosa de la seguridad de la información: "a) política de seguridad, objetivos y actividades que reflejen los objetivos de la empresa; b) una estrategia de implementación de seguridad que sea consecuente con la cultura de la organización; c) apoyo y compromiso manifiesto por parte de la gerencia; d) un claro enten-

dimiento de los requerimientos de seguridad, la evaluación de riesgos y la administración de los mismos; e) comunicación eficaz de los temas de seguridad a todos los gerentes y demás empleados; f) distribución de guías sobre políticas y normas de seguridad de la información a todos los empleados y contratistas; g) instrucción y entrenamiento adecuados; h) un sistema integral y equilibrado de medición que se utilice para evaluar el desempeño de la gestión de la seguridad de la información y para brindar sugerencias tendientes a mejorarlo";

- el estándar "puede ser considerado como un punto de partida para el desarrollo de lineamientos específicos, aplicables a cada organización".

Áreas de control.

Este estándar detallado de la seguridad, IRAM-ISO/IEC 17799, se organiza en 10 (diez) Áreas de control esenciales.

Los organismos respectivos que tuvieron a cargo su estudio han sido los siguientes:

- Subcomité de Seguridad de la Información;
- Comité General de Normas (CGN)

Los integrantes de dicho Subcomité representaron al IRAM, Colegio de Abogados, ISACA (*Information Systems Audit And Control Association*), IEEE Argentina, Secretaría de Modernización del Estado, Ministerio de Justicia y Derechos Humanos y Universidad Tecnológica Nacional (Fac. Reg. Bs. As.). Como se puede apreciar, los CPCE y la FACPCE no estuvieron representados.

Objetivos de control y controles para alcanzarlos.

Estas áreas de control clave, a su vez, contienen 36 (treinta y seis) Objetivos de Control, y 139 (ciento treinta y nueve) Controles para alcanzarlos.

La descripción siguiente no reemplaza la lectura pormenorizada de la norma:

2.1. Política de seguridad (*Security Policy*).

Se precisa una política que refleje las expectativas de la organización en materia de seguridad a fin de suministrar administración con dirección y soporte, pudiéndose también utilizar como la base para el estudio y evaluación en curso: "Objetivo: política de seguridad de la información: proporcionar dirección y apoyo gerencial para brindar seguridad de la información. El nivel gerencial debe establecer una dirección política clara y demostrar apoyo y compromiso con respecto a la seguridad de la información, mediante la formulación y mantenimiento de una política de seguridad de la información a través de toda la organización".

* Documentación de la política de seguridad de la información (*Information Security Policy Document*)

Los responsables gerenciales deben aprobar y publicar la política de seguridad y comunicarla al personal, que contenga como mínimo pautas sobre: a) definición de la seguridad de la información, objetivos, alcance e importancia; b) declaración del propósito del nivel gerencial, apoyando los objetivos y principios; c) breve explicación de las políticas, principios, normas y requisitos de cumplimiento en materia de seguridad; d) definición de las responsabilidades generales y específicas, incluyendo la comunicación de los incidentes; e) referencias a otros documentos que respaldan la política.

* Revisión y evaluación (*Review and Evaluation*)

La política debe tener un responsable del mantenimiento y revisión de acuerdo con el proceso definido, y deben programarse revisiones periódicas de: a) la eficacia demostrada por la política; b) el costo e impacto de los controles en la eficiencia; c) los efectos de modificaciones en la tecnología.

2.2. Organización de la seguridad (*Organizational Security*).

Se sugiere diseñar una estructura de administración dentro del ente que establezca la responsabilidad de los grupos en ciertas áreas de seguridad y un proceso para el manejo de la respuesta a incidentes; así como aspectos de seguridad

frente al acceso por parte de terceros y la tercerización del procesamiento de información: 1. "Objetivo: infraestructura de seguridad de la información: administrar la seguridad de la información dentro de la organización. Debe establecerse un marco gerencial para iniciar y controlar la implementación de la seguridad de la información dentro de la organización. Deben establecerse adecuados foros de discusión liderados por niveles gerenciales, a fin de aprobar la política de seguridad de la información, asignar funciones de seguridad y coordinar la implementación de la seguridad en toda la organización. Si resulta necesario, se debe establecer y hacer accesible dentro de la organización una fuente de asesoramiento especializado en materia de seguridad de la información. Deben desarrollarse contactos con especialistas externos en materia de seguridad para estar al corriente de las tendencias de la industria, monitorear estándares y métodos de evaluación y proveer puntos de enlace adecuados al afrontar incidentes de seguridad. Se debe alentar la aplicación de un enfoque multidisciplinario de la seguridad de la información, por ejemplo, comprometiendo la cooperación y colaboración de gerentes, y expertos en áreas como seguros y administración de riesgos."; 2. "Objetivo: seguridad frente al acceso por parte de terceros: mantener la seguridad de las instalaciones de procesamiento de información y de los recursos de información de la organización a los que acceden terceras partes. Se debe controlar el acceso a las instalaciones de procesamiento de información de la organización por parte de terceros. Cuando existe una necesidad de la empresa para permitir dicho acceso, debe llevarse a cabo una evaluación de riesgos para determinar las incidencias en la seguridad y los requerimientos de control. Los controles deben ser acordados y definidos en un contrato con la tercera parte. El acceso de terceros también puede involucrar otros participantes. Los contratos que confieren acceso a terceros deben incluir un permiso para la designación de otros participantes capacitados y las condiciones para su acceso. Este estándar puede utilizarse como base para tales contratos y cuando se considere la tercerización del procesamiento de información."; 3. "Objetivo: tercerización: mantener la seguridad de la información cuando la responsabilidad por el procesamiento de la misma fue asignada a otra organización. Los acuerdos de tercerización deben contemplar los riesgos, los controles de seguridad y los procedimientos para sistemas de información, redes y/o ambientes de PC (*desk top environments*) en el contrato entre las partes".

Infraestructura de seguridad de la información (Information Security Infrastructure).

* Foro gerencial sobre seguridad de la información (*Management Information Security Forum*)

Debe crearse un foro gerencial para garantizar la clara dirección y apoyo a las iniciativas de seguridad, que debe promover la seguridad dentro de la organización y comprende las acciones de: a) revisar y aprobar la política y responsabilidades generales en la materia; b) monitorear los cambios significativos de la exposición de la información frente a las amenazas; c) revisar los incidentes que se produzcan; d) aprobar las iniciativas para incrementar la seguridad de la información.

* Coordinación de la seguridad de la información (*Information Security Coordination*)

Podría ser conveniente, la creación de un foro interfuncional que comprenda a los representantes de la gerencia de sectores importantes de una gran organización para coordinar la implementación de controles que: a) acuerde funciones y responsabilidades específicas; b) determine metodologías y procesos específicos; c) brinde apoyo a las iniciativas de seguridad; d) garantice que la seguridad integre el proceso de planificación de la información; e) evalúe y coordine la implementación de controles específicos; f) controle incidentes relativos al tema; g) promueva la difusión del apoyo de la empresa a la seguridad de la información.

* Asignación de responsabilidades en materia de seguridad de la información (*Allocation of Information Security Responsibilities*)

Deben definirse las responsabilidades para la protección de los recursos y para la implementación de procesos específicos de seguridad, siendo clave que se establezcan las áreas sobre las cuales es responsable cada gerente, debiendo: a) identificarse y definirse los diversos recursos y procesos de seguridad relacionados con los diferentes sistemas; b) designarse al gerente responsable de cada recurso y proceso de seguridad, documentando sus detalles; c) determinarse los niveles de autorización claramente documentados.

* Proceso de autorización para instalaciones de procesamiento de información (*Authorization Process for Information Processing Facilities*)

Corresponde establecer un proceso de autorización gerencial para las nuevas instalaciones de procesamiento de información, considerando que: a) deben ser aprobadas por la gerencia usuaria, autorizando su propósito y uso; b) debe verificarse el hardware y software garantizando que sean compatibles con las partes de otros sistemas; c) tiene que ser autorizado el uso de las instalaciones personales para el procesamiento de información de la empresa, así como los controles del caso; d) dichas instalaciones personales de procesamiento de información en el sitio de trabajo puede causar vulnerabilidades, por lo que debe ser evaluado y autorizado.

* Asesoramiento especializado en materia de seguridad de la información (*Specialist Information Security Advice*)

Muchas organizaciones probablemente requieran de asesoramiento especializado en materia de seguridad e idealmente debe ser provisto por un asesor interno experimentado en seguridad de la información, o identificando a una persona determinada para coordinar los conocimientos y experiencias de la organización; pudiéndose tener acceso a asesores externos apropiados.

* Cooperación entre organizaciones (*Cooperation between Organizations*)

Deben mantenerse contactos adecuados con autoridades policiales o de seguridad, organismos reguladores, proveedores de servicios de información y operadores de telecomunicaciones, con el fin de garantizar que, ocurrido un incidente determinado, puedan tomarse las medidas adecuadas y lograrse asesoramiento inmediato, pero garantizando que no se divulgue información confidencial.

* Revisión independiente de la seguridad de la información (*Independent Review of Information Security*)

Debe ser revisada con independencia la implementación del documento que fija la política de seguridad, para garantizar que las prácticas de la organización reflejan dicha política y que la misma es viable y efectiva, pudiéndose ser

realizado por la función de auditoría interna, por un gerente independiente o una organización externa especializada.

Seguridad frente al acceso por parte de terceros (Security of Third Party Access).

* Identificación de riesgos del acceso de terceras partes (*Identification of Risks from Third Party Access*)

- Tipos de acceso (*Types of Access*)

Los tipos de acceso otorgado a terceras partes es de importancia, existiendo riesgos distintos tales como el acceso a través de una conexión de red o los relativos al acceso físico: a) acceso físico (oficinas, salas de cómputos, armarios); b) acceso lógico (bases de datos y sistemas de información).

- Razones para el acceso (*Reasons for Access*)

Existen terceros que proveen servicios al ente y se les puede otorgar acceso físico y lógico por distintas razones: a) personal de soporte de hardware y software; b) socios comerciales o con riesgos compartidos, por lo que la información puede ponerse en riesgo si dicho acceso se realiza en el contexto de una inadecuada administración de la seguridad, por lo que deben evaluarse los riesgos para identificar los requerimientos de controles específicos.

- Contratistas (*On-Site Contractors*)

Las terceras partes ubicadas en la entidad por un tiempo determinado según contrato, también pueden originar debilidades en materia de seguridad: a) personal de mantenimiento y soporte; b) limpieza, servicio de comida, guardia de seguridad y otros servicios tercerizados; c) pasantías y otras designaciones de corto plazo; d) consultores y otros; siendo esencial determinar los controles necesarios para administrar el acceso a las instalaciones de procesamiento de información.

* Requerimientos de seguridad en contratos con terceros (*Security Requirements in Third Party Contracts*)

Debe existir un contrato formal que contemple el acceso de terceros a las

instalaciones de procesamiento de información del ente, conteniendo los requerimientos de seguridad con el objetivo de asegurar el cumplimiento de políticas y estándares, con cláusulas tales como: a) política general de seguridad de la información; b) protección de activos; c) descripción de cada servicio; d) nivel de servicio aspirado; e) disposición contemplando la transferencia de personal cuando corresponda; f) obligaciones de las partes; g) responsabilidades con relación a asuntos legales; h) derechos de propiedad intelectual; i) acuerdos de control de acceso; j) definición de criterios de desempeño; k) derecho de monitorear y revocar la actividad; l) derecho a auditar las responsabilidades contractuales; m) establecimiento de un proceso para la resolución de problemas; n) responsabilidades relativas a la instalación y mantenimiento de hardware y software; o) estructura de dependencia y del proceso de informes; p) proceso de administración de cambios; q) controles de protección física y mecanismos de implementación; r) métodos y procedimientos de entrenamiento de usuarios; s) controles para la protección contra software malicioso; t) disposiciones para informes, incidentes y violaciones de la seguridad; u) relación entre proveedores y subcontratistas.

Tercerización (Outsourcing).

* Requerimientos de seguridad en contratos de tercerización (*Security Requirements in Outsourcing Contracts*)

Las necesidades de seguridad de un ente que terceriza la administración y el control de sus sistemas de información deben ser consideradas en un contrato acordado entre las partes que contemple: a) requisitos legales; b) conocimiento de las responsabilidades; c) integridad y confidencialidad de los activos del negocio; d) controles para el acceso de los usuarios autorizados a la información; e) mantenimiento de la disponibilidad de los servicios en caso de desastres; f) niveles de seguridad física asignados al equipamiento tercerizado; g) derecho a la auditoría.

2.3. Clasificación y control de activos (*Asset Classification and Control*).

Se necesita de un inventario de los recursos de información de la organi-

zación y con base a este conocimiento, se debería brindar un nivel adecuado de protección: 1. "Objetivo: responsabilidad por rendición de cuentas de los activos: mantener una adecuada protección de los activos de la organización. Se debe rendir cuentas por todos los recursos de información importantes y se debe designar un propietario para cada uno de ellos. La rendición de cuentas por los activos ayuda a garantizar que se mantenga una adecuada protección. Se deben identificar a los propietarios para todos los activos importantes y de asignarse la responsabilidad por el mantenimiento de los controles adecuados. La autoridad por la implementación de los controles puede ser delegada, creándose la responsabilidad correspondiente. En último término, el propietario designado del activo debe rendir cuentas por el mismo"; 2. "Objetivo: clasificación de la información: garantizar que los recursos de información reciban un apropiado nivel de protección. La información debe ser clasificada para señalar la necesidad, las prioridades y el grado de protección. La información tiene diversos grados de sensibilidad y criticidad. Algunos ítem pueden requerir un nivel de protección adicional o un tratamiento especial. Se debe utilizar un sistema de clasificación de la información para definir un conjunto apropiado de niveles de protección y comunicar la necesidad de medidas de tratamiento especial".

Responsabilidad por rendición de cuentas de los activos (Accountability For Assets).

* Inventario de activos (*Inventory of Assets*)

Los inventarios de activos colaboran en avalar un resguardo efectivo de los recursos y además, pueden ser necesarios para fines vinculados con sanidad y seguridad, seguros o finanzas, debiéndose mantener un inventario de los activos importantes asociados a cada sistema de información: a) recursos de información (bases de datos y archivo, documentación de sistemas, manuales de usuario, material de capacitación, entre otros); b) recursos de software (de aplicaciones, de sistemas, herramientas de desarrollo y utilitarios), c) activos físicos (equipamiento informático, equipos de comunicaciones, medios magnéticos, mobiliario, etc.); d) servicios (informáticos y de comunicaciones, utilitarios generales).

Clasificación de la información (Information Classification).

* Pautas de clasificación (*Classification Guidelines*)

Las clasificaciones (forma de tratamiento) y controles de protección de la información, deben considerar las necesidades de la organización con relación a su distribución o restricción, y la incidencia en las actividades. La información y las salidas de sistemas deben ser rotuladas según su valor y grado de sensibilidad para el ente.

* Rotulado y manejo de la información (*Information Labelling and Handling*)

Deben definirse los procedimientos para el etiquetado y manejo de la información, conforme al esquema de clasificación adoptado por la empresa, considerando los tipos de actividades de procesamiento de la información: a) copia; b) almacenamiento; c) transmisión por correo, fax y correo electrónico; d) transmisión oral (telefonía, correo de voz, contestadores automáticos).

2.4. Seguridad del personal (*Personnel Security*).

Se establece la necesidad de educar e informar a los empleados actuales y potenciales acerca de lo que se espera de ellos en materia de seguridad y asuntos de confidencialidad. También, determina cómo incide el rol que desempeña el personal en materia de seguridad en el funcionamiento general de la entidad, debiéndose implementar un plan para informar los incidentes: 1. "Objetivo: seguridad en la definición de puestos de trabajo y la asignación de recursos: reducir los riesgos de error humano, robo, fraude o uso inadecuado de instalaciones. Las responsabilidades en materia de seguridad deben ser explicitadas en la etapa de reclutamiento, incluidas en los contratos y monitoreadas durante el desempeño del individuo como empleado. Los candidatos a ocupar los puestos de trabajo deben ser adecuadamente seleccionados, especialmente si se trata de tareas críticas. Todos los empleados y usuarios externos de las instalaciones de procesamiento de información deben firmar un acuerdo de confidencialidad"; 2. "Objetivo: capacitación del usuario: garantizar que los usuarios están al corriente de las amenazas e incumbencias en materia de seguridad de la información, y están capacitados para respaldar la política de se-

guridad de la organización en el transcurso de sus tareas normales. Los usuarios deben ser capacitados en relación con los procedimientos de seguridad y el correcto uso de las instalaciones de procesamiento de información, a fin de minimizar eventuales riesgos de seguridad", 3. "Objetivo: respuesta a incidentes y anomalías en materia de seguridad: minimizar el daño producido por incidentes y anomalías en materia de seguridad, y monitorear dichos incidentes y aprender de los mismos. Los incidentes que afectan la seguridad deben ser comunicados mediante canales gerenciales adecuados tan pronto como sea posible. Se debe concientizar a todos los empleados y contratistas acerca de los procedimientos de comunicación de los diferentes tipos de incidentes (violaciones, amenazas, debilidades o anomalías en materia de seguridad) que podrían producir un impacto en la seguridad de los activos de la organización. Se debe requerir que los mismos comuniquen cualquier incidente advertido o supuesto al punto de contacto designado tan pronto como sea posible. La organización debe establecer un proceso disciplinario formal para ocuparse de los empleados que perpetren violaciones de la seguridad. Para lograr abordar debidamente los incidentes podría ser necesario recolectar evidencia tan pronto como sea posible una vez ocurrido el hecho".

Seguridad en la definición de puestos de trabajo y la asignación de recursos (Security in Job Definition and Resourcing).

* Inclusión de la seguridad en las responsabilidades de los puestos de trabajo (*Including Security in Job Responsibilities*)

Las funciones y responsabilidades por la seguridad (implementación o mantenimiento de la política, obligaciones específicas por la protección de activos, ejecución de procesos o actividades), conforme a la política de seguridad, deben ser documentadas según corresponda.

* Selección y política de personal (*Personnel Screening and Policy*)

Cuando se solicita el puesto (personas que tienen acceso a las instalaciones de procesamiento de información y en particular, si éstas manejan información sensible) se deben practicar controles de verificación del personal permanente, que incluyan: a) certificados de buena conducta; b) comprobación del

curriculum vitae; c) comprobación de aptitudes; d) verificación de la identidad. Un proceso similar debe llevarse a cabo con contratistas y personal temporario. El trabajo de todo el personal debe ser pasible de revisión periódica y a procedimientos de aprobación por parte de miembros con mayor jerarquía.

* Acuerdos de confidencialidad (*Confidentiality Agreements*)

Los empleados deben firmar un acuerdo de confidencialidad o no divulgación, como parte de los términos y condiciones iniciales de empleo, para confirmar que la información es confidencial o secreta. El personal ocasional y los usuarios externos también deberán firmar el acuerdo antes de que se les permita el acceso a las instalaciones de procesamiento de la información.

* Términos y condiciones de empleo (*Terms and Conditions of Employment*)

Los términos y condiciones de empleo deben establecer la responsabilidad del personal por la seguridad de la información, incluyendo las acciones que puedan corresponder.

Capacitación del usuario (User Training).

* Formación y entrenamiento en materia de seguridad de la información (*Information Security Education and Training*)

Todos los empleados de la empresa, y en su caso, los usuarios externos deben tener una capacitación y actualizaciones periódicas en materia de políticas y procedimientos de la organización, comprendiendo los requerimientos de seguridad, responsabilidades legales, controles del negocio, uso de las instalaciones de procesamiento de información.

Respuesta a incidentes y anomalías en materia de seguridad (Responding to Security Incidents and Malfunctions).

* Comunicación de incidentes relativos a la seguridad (*Reporting Security Incidents*)

Los incidentes vinculados con la seguridad deben comunicarse por medio de los canales gerenciales apropiados ni bien sea posible, mediante un proceso

formal de comunicación, junto con un procedimiento de respuesta a sucesos, estableciendo la acción a emprender al recibir un informe sobre el particular.

* Comunicación de debilidades en materia de seguridad (*Reporting Security Weaknesses*)

Los usuarios de servicios de información deben determinar, registrar y comunicar las debilidades o amenazas probables u observadas en materia de seguridad, con relación a los sistemas o los servicios, comunicando estos asuntos a su gerencia, o al proveedor de servicios.

* Comunicación de anomalías del software (*Reporting Software Malfunctions*)

Se deben establecer los procedimientos para la comunicación de anormalidades del software, considerando como acciones: a) advertencia y registro de los síntomas del problema; b) aislamiento de la computadora o detenerse su uso; c) comunicación inmediata al gerente de seguridad de la información.

* Aprendiendo de los incidentes (*Learning from Incidents*)

La información resultante de la implementación de mecanismos que permitan cuantificar y monitorear los tipos, volúmenes y costos de los incidentes y anomalías, debe utilizarse para identificar estos problemas recurrentes o de alto impacto, pudiendo señalar la necesidad de mejorar o agregar controles.

* Proceso disciplinario (*Disciplinary Process*)

Debe haber un proceso disciplinario formal para los empleados que vulneren las políticas y procedimientos de seguridad de la organización.

2.5. Seguridad Física y Ambiental (*Physical and Environmental Security*).

Responde a la exigencia de proteger las áreas, el equipo y los controles generales: 1. "Objetivo: áreas seguras: impedir accesos no autorizados, daños e interferencia a las sedes e información de la empresa. Las instalaciones de procesamiento de información crítica o sensible de la empresa deben estar ubicadas en áreas protegidas y resguardadas por un perímetro de seguridad definido, con vallas de seguridad y controles de acceso apropiados. Deben estar

fisicamente protegidas contra accesos no autorizados, daños e intrusiones. La protección provista debe ser proporcional a los riesgos identificados. Se recomienda la implementación de políticas de escritorios y pantallas limpios para reducir el riesgo de acceso no autorizado o de daño a papeles, medios de almacenamiento e instalaciones de procesamiento de información"; 2. "Objetivo: seguridad del equipamiento: impedir pérdidas, daños o exposiciones al riesgo de los activos e interrupción de las actividades de la empresa. El equipamiento debe estar fisicamente protegido de las amenazas a la seguridad y los peligros del entorno. Es necesaria la protección del equipamiento (incluyendo el que se utiliza en forma externa) para reducir el riesgo de acceso no autorizado a los datos y para prevenir pérdidas o daños. Esto también debe tener en cuenta la ubicación y disposición del equipamiento. Pueden requerirse controles especiales para prevenir peligros o accesos no autorizados, y para proteger instalaciones de soporte, como la infraestructura de cableado y suministro de energía eléctrica"; y 3. Objetivo: controles generales: impedir la exposición al riesgo o robo de la información o de las instalaciones de procesamiento de la misma. Las instalaciones de procesamiento de la información y la información deben ser protegidas contra la divulgación, modificación o robo por parte de personas no autorizadas, debiéndose implementar controles para minimizar pérdidas o daños. Los procedimientos de administración y almacenamiento son considerados...".

Áreas seguras (Security Areas).

* Perímetro de seguridad física (*Physical Security Perimeter*)

La protección física puede concretarse mediante diversas barreras físicas alrededor de las sedes de la entidad y de las instalaciones de procesamiento de la información, que establezcan un perímetro de seguridad, claramente definido, para incrementar la protección total provista.

* Controles de acceso físico (*Physical Entry Controls*)

Las áreas protegidas deben estar resguardadas por controles de acceso que garanticen que solamente se permite el acceso a personal autorizado.

* Protección de oficinas, recintos e instalaciones (*Securing Offices, Rooms and Facilities*)

Un área protegida, que debe seleccionarse y diseñarse teniendo en cuenta la posibilidad de daño producido por varias formas de desastres naturales o provocados por el hombre, puede consistir en una oficina cerrada con llave, o diversos lugares dentro de un perímetro de seguridad física, que puede estar bloqueado y contener cajas fuertes o gabinetes con cerradura.

* Desarrollo de tareas en áreas protegidas (*Working in Secure Areas*)

Para aumentar la seguridad de un área protegida pueden necesitarse controles y lineamientos adicionales, que incluye los controles para el personal o terceras partes que trabajan en dicha área, así como las actividades de terceros.

* Aislamiento de las áreas de entrega y carga (*Insolated Delivery and Loading Areas*)

Las áreas de entrega y carga deben ser controladas, y en su caso, aisladas de las instalaciones de procesamiento de información, para impedir accesos no autorizados, y sus requerimientos de seguridad deben ser determinados mediante una evaluación de riesgos.

Seguridad del equipamiento (Equipment Security).

* Ubicación y protección del equipamiento (*Equipment Siting and Protection*)

El equipamiento debe ser ubicado de forma tal que se reduzcan los riesgos ocasionados por amenazas, peligros ambientales y oportunidades de acceso no autorizado.

* Suministro de energía (*Power Supplies*)

El equipamiento tiene que estar protegido con respecto a las posibles fallas en el suministro de energía u otros problemas eléctricos y considerarse alternativas para asegurar la continuidad del dicho suministro: a) múltiples bocas de suministro; b) suministro de energía no interrumpible; c) generador de respaldo.

* Seguridad del cableado (*Cabling Security*)

El cableado de energía eléctrica y de comunicaciones que transporta datos o brinda respaldo a los servicios de información debe ser protegido contra interceptación o daño.

* Mantenimiento de equipos (*Equipment Maintenance*)

El equipamiento debe mantenerse en forma apropiada para asegurar su disponibilidad e integridad permanente.

* Seguridad del equipamiento fuera del ámbito de la organización (*Security of Equipment Off-Premises*)

La utilización de equipamiento para el procesamiento de información, fuera del lugar físico de la empresa, debe ser autorizado por el nivel gerencial.

* Baja segura o reutilización de equipamiento (*Secure Disposal or Re-use of Equipment*)

Se debe evitar que la información pueda verse comprometida por una desafectación descuidada o una reutilización del equipamiento.

Controles generales (General Controls).

* Políticas de escritorios y pantallas limpias (*Clear Desk and Clear Screen Policy*)

Las empresas deben adoptar una política de escritorios limpios para proteger documentos en papel y dispositivos de almacenamiento removibles, y una política de pantallas limpias en las instalaciones de procesamiento de información, para disminuir los riesgos de acceso no autorizado y pérdida o daño de la información.

* Retiro de bienes (*Removal of Property*)

El equipamiento, la información o el software no deben ser retirados de la sede del ente sin autorización, y se deben concretar comprobaciones puntuales.

2.6. Gestión de comunicaciones y operaciones (*Communications and Operations Management*).

Los objetivos de esta sección consisten en: a) reforzar el funcionamiento correcto y seguro de las instalaciones de procesamiento de la información; b) minimizar el riesgo de fallas de los sistemas; c) proteger la integridad del software y la información; d) conservar la totalidad y disponibilidad del procesamiento y la comunicación de la información; e) garantizar la protección de la información en las redes y de la infraestructura de apoyo; f) evitar daños a los recursos de información e interrupciones en las actividades de la compañía; y g) evitar la pérdida, modificación o uso indebido de la información que intercambian las organizaciones: 1. "Objetivo Procedimientos y responsabilidades operativas: garantizar el funcionamiento correcto y seguro de las instalaciones de procesamiento de la información. Se deben establecer las responsabilidades y procedimientos para la gestión y operación de todas las instalaciones de procesamiento de información. Esto incluye el desarrollo de instrucciones operativas y procedimientos apropiados de respuesta a incidentes. Se debe implementar la separación de funciones, cuando corresponda, a fin de reducir el riesgo del uso negligente o mal uso deliberado del sistema"; 2. "Objetivo: planificación y aprobación de sistemas: minimizar el riesgo de fallas en los sistemas. Se requiere una planificación y preparación anticipada para garantizar la disponibilidad de capacidad y recursos adecuados. Deben realizarse proyecciones para futuros requerimientos de capacidad, a fin de reducir el riesgo de sobrecarga del sistema. Se deben establecer, documentar y probar los requerimientos operativos de nuevos sistemas antes de su aprobación y uso"; 3. "Objetivo: protección contra software malicioso: proteger la integridad del software y la información. Es necesario tomar precauciones para prevenir y detectar la introducción de software malicioso. El software y las instalaciones de procesamiento de información son vulnerables a la introducción de software malicioso como, por ejemplo, virus informático, *worms* de red, troyanos y bombas lógicas. Se debe concientizar a los usuarios acerca de los peligros del software no autorizado o malicioso, y los administradores deben, cuando corresponda, introducir los controles especiales para detectar o prevenir la introducción de los mismos. En particular, es esencial que se tomen precauciones

para detectar y prevenir virus informáticos en computadoras personales"; 4. "Objetivo: mantenimiento: mantener la integridad y disponibilidad de los servicios de procesamiento y comunicación de información. Se deben establecer procedimientos de rutina para llevar a cabo la estrategia de resguardo acordada realizando copias de resguardo de los datos y ensayando su restablecimiento oportuno, registrando eventos y fallas y, cuando corresponda, monitoreando el entorno del equipamiento"; 5. "Objetivo: administración de la red: garantizar la seguridad de la información en las redes y la protección de la infraestructura de apoyo. Es de suma importancia la administración de seguridad de las redes que pueden atravesar el perímetro de la organización. También pueden requerirse controles adicionales para los datos sensibles que circulen por redes públicas"; 6. "Objetivo: administración y seguridad de los medios de almacenamiento: impedir el daño a los activos y las interrupciones en las actividades de la organización. Los medios de almacenamiento deben ser controlados y protegidos físicamente. Se deben establecer procedimientos operativos apropiados para proteger documentos, medios de almacenamiento (cintas, discos, casetes), datos de entrada/salida y documentación del sistema contra daño, robo y acceso no autorizado"; 7. "Objetivo: intercambios de información y software: impedir la pérdida, modificación o uso inadecuado de la información que intercambian las organizaciones. Los intercambios de información y software entre organizaciones deben ser controlados, y deben ser consecuentes con la legislación aplicable. Los intercambios deben llevarse a cabo de conformidad con los acuerdos existentes. Se deben establecer procedimientos y normas para proteger la información y los medios en tránsito. Se deben considerar las implicancias comerciales y de seguridad relacionadas con el intercambio electrónico de datos, el comercio electrónico y el correo electrónico, además de los requerimientos de controles".

Procedimientos y responsabilidades operativas (Operational Procedures and Responsibilities).

* Documentación de los procedimientos operativos (*Documented Operating Procedures*)

Se deben documentar y mantener los procedimientos operativos individua-

lizados en la política de seguridad, los que deben ser tratados en documentos formales y con los cambios autorizados por nivel gerencial.

* Control de cambios en las operaciones (*Operational Change Control*)

Deben controlarse los cambios en los sistemas e instalaciones de procesamiento de información, puesto que su omisión es una causa común de las fallas de seguridad y de sistemas.

* Procedimientos de manejo de incidentes (*Incident Management Procedures*)

Se deben implementar responsabilidades y procedimientos de manejo de incidentes para asegurar una respuesta oportuna, efectiva y sistemática a los incidentes relativos a seguridad.

* Separación de funciones (*Segregation of Duties*)

La segregación de funciones en un método para reducir el riesgo de mal uso del sistema, debiéndose considerar la separación de la gestión o ejecución de las tareas o áreas de responsabilidad, a fin de minimizar las oportunidades de modificación sin autorización o uso incorrecto de la información o los servicios. Cuando sea difícil concretar la separación, deben considerarse otros controles, como el monitoreo de actividades, las pistas de auditoría y la supervisión gerencial.

* Separación entre instalaciones de desarrollo e instalaciones operativas (*Separation of Development and Operational Facilities*)

La segregación entre las instalaciones de desarrollo, prueba y operaciones es necesaria para obtener la separación de los roles involucrados, debiéndose definir y documentar las reglas para la transferencia del software desde la situación de desarrollo hacia el estado operativo.

* Administración de instalaciones externas (*External Facilities Management*)

El uso de un contratista externo para la administración de las instalaciones de procesamiento de información puede provocar probables exposiciones al riesgo en materia de seguridad, como ser la posibilidad de daño o pérdida de los datos en la sede del contratista, por lo que estos riesgos deben ser identifi-

cados con anticipación y acordarse controles adecuados a incluirse en el contrato.

Planificación y aprobación de sistemas (System Planning and Acceptance).

* Planificación de la capacidad (*Capacity Planning*)

Se deben controlar las demandas de capacidad y realizar proyecciones de los requerimientos futuros, con el objetivo de garantizar la disponibilidad del procesamiento y almacenamiento adecuados, teniendo en consideración las nuevas necesidades de negocios y sistemas, y las tendencias en el procesamiento de la información de la organización.

* Aprobación del sistema (*System Acceptance*)

Se deben determinar criterios de aprobación, claramente definidos, acordados, documentados y probados, para los nuevos sistemas de información, actualizaciones y nuevas versiones, y llevarse a cabo pruebas de los sistemas antes de su aprobación.

Protección contra software malicioso (Protection against Malicious Software).

* Controles contra software malicioso (*Controls against Malicious Software*)

Se deben implementar controles, detectivos y preventivos, para la protección contra programas maliciosos y procedimientos de implicación de usuarios en materia de seguridad, incluyendo controles adecuados de acceso al sistema y administración de cambios.

Mantenimiento (Housekeeping).

* Resguardo de la información (*Information Back-Up*)

Se deben efectuar periódicamente copias de resguardo de la información y el software imprescindibles para la organización.

* Registro de actividades del personal operativo (*Operator Logs*)

El personal operativo debe mantener un registro de sus actividades que in-

cluya: a) tiempos de inicio y cierre del sistema; b) errores del sistema y medidas correctivas; c) confirmación del manejo adecuado de archivos de datos y salidas; d) nombre de la persona que actualiza el registro.

* Registro de fallas (*Fault Logging*)

Se deben comunicar las fallas con respecto a problemas con el procesamiento de la información o los sistemas de comunicaciones, y concretar las medidas correctivas.

Administración de la red (Network Management).

* Controles de redes (*Network Controls*)

Se necesita un conjunto de controles para obtener y mantener la seguridad de las redes informáticas, que deben ser implementados por los administradores de redes para garantizar la seguridad de los datos y la protección de los servicios conectados contra el acceso no autorizado.

Administración y seguridad de los medios de almacenamiento (Media Handling and Security).

* Administración de medios informáticos removibles (*Management of Removable Computer Media*)

Deben existir procedimientos y niveles de autorización documentados para la administración de medios informáticos removibles (cintas, discos, casetes e informes impresos).

* Eliminación de medios informáticos (*Disposal of Media*)

Los medios informáticos, cuando ya no sean requeridos, deben eliminarse en forma segura, para evitar que la información sensible pueda filtrarse a personas ajenas a la organización. Los ítem que pueden precisar una eliminación son: documentos en papel, grabaciones, papel carbónico, informes de salida, cintas de impresora, cintas magnéticas, discos o casetes, medios de almacenamiento óptico, listados de programas, datos de prueba, documentación del sistema, etcétera.

* Procedimientos de manejo de la información (*Information Handling Procedures*)

Deben establecerse procedimientos para el manejo y almacenamiento de la información para su protección contra el uso inadecuado o la divulgación no autorizada.

* Seguridad de la documentación del sistema (*Security of System Documentation*)

La documentación del sistema puede contener información sensible, tal como descripción de procesos de aplicaciones, procedimientos, estructuras de datos, procesos de autorización, debiéndose considerar controles para protegerla de accesos no autorizados.

Intercambios de información y software (Exchanges of Information and Software).

* Acuerdos de intercambio de información y software (*Information and Software Exchange Agreements*)

Se deben crear acuerdos para el intercambio de información y programas entre organizaciones, los que deben reflejar el grado de sensibilidad de la información del negocio involucrada.

* Seguridad de los medios en tránsito (*Security of Media in Transit*)

La información puede ser vulnerable a accesos no autorizados, mal uso o alteración durante el transporte físico (servicios postales o mensajería), debiéndose aplicar controles para salvaguardar los medios informáticos que se transportan entre distintos lugares.

* Seguridad del comercio electrónico (*Electronic Commerce Security*)

El comercio electrónico puede incluir el uso de intercambio electrónico de datos (EDI), correo electrónico, y transacciones en línea por medio de redes públicas como Internet, siendo vulnerable a varias amenazas relativas a redes, que pueden resultar en actividades fraudulentas, controversias contractuales y divulgación o modificación de información, por lo que se deben aplicar controles para protegerlo de dichas amenazas.

* Seguridad del correo electrónico

- Riesgos de seguridad y política de correo electrónico (*Security of Electronic Mail: Security Risks; Policy on Electronic Mail*)

El correo electrónico se está empleando para las comunicaciones comerciales, en reemplazo de las informaciones vía telex y correo postal, difiriendo de estas formas tradicionales por su velocidad, estructura de mensajes, grado de informalidad y vulnerabilidad a acciones no autorizadas, debiéndose tener en cuenta controles para reducir los riesgos de seguridad creados por su utilización.

Las organizaciones deben confeccionar una política con relación al uso del correo electrónico que incluya: a) ataques al mismo; b) protección de archivos adjuntos; c) lineamientos sobre cuándo no utilizarlo; d) responsabilidades del empleado de no comprometer a la organización; e) uso de técnicas criptográficas; f) retención de mensajes; g) controles adicionales para mensajes no autenticados.

* Seguridad de los sistemas electrónicos de oficina (*Security of Electronic Office Systems*)

Se deben preparar e implementar políticas y lineamientos para controlar las actividades de la organización y riesgos de seguridad con respecto a los sistemas electrónicos de oficina, que propician la difusión y distribución de la información, mediante una combinación de documentos, computadoras, computación móvil, comunicaciones móviles, correo, comunicaciones de voz, multimedia y máquinas de fax, entre otros.

* Sistemas de acceso público (*Publicly Available Systems*)

Deben tomarse recaudos para la protección de la integridad de la información publicada en forma electrónica, para prevenir la modificación no autorizada que podría perjudicar la reputación de la organización.

* Otras formas de intercambio de información (*Others Forms of Information Exchange*)

Se deben implementar procedimientos y controles para proteger el intercambio de información a través de medios de comunicaciones de voz, fax y video.

2.7. Control de accesos (*Access Control*).

Se instala la importancia de los requerimientos para monitorear los accesos; la administración de accesos de usuarios; las responsabilidades de los mismos; el control del acceso a la red, al sistema operativo y las aplicaciones, y la seguridad de la información por computación móvil y trabajo remoto, contra los abusos internos e intrusos externos: 1. "Objetivo: requerimientos de negocio para el control de accesos: controlar el acceso de información. El acceso a la información y los procesos de negocio deben ser controlados sobre la base de los requerimientos de seguridad y de los negocios. Para ésta se deben tener en cuenta las políticas de difusión y autorización de la información.", 2. Objetivo: administración de accesos de usuarios: impedir el acceso no autorizado en los sistemas de información. Se deben implementar procedimientos formales para controlar la asignación de derechos de acceso a los sistemas y servicios de información. Los procedimientos deben comprender todas las etapas del ciclo de vida de los accesos de usuarios, desde el registro inicial de nuevos usuarios hasta la privación final de derechos de los usuarios que ya no requieran acceso a los sistemas y servicios de información. Se debe conceder especial atención, cuando corresponda, a la necesidad de controlar la asignación de derechos de acceso de privilegio, que permiten a los usuarios pasar por alto los controles de sistema"; 3. "Objetivo: responsabilidades del usuario: impedir el acceso a usuarios no autorizados. La cooperación de los usuarios autorizados es esencial para la eficacia de la seguridad. Se debe concientizar a los usuarios acerca de sus responsabilidades por el mantenimiento de controles de acceso eficaces, en particular aquellos relacionados con el uso de contraseñas y la seguridad del equipamiento"; 4. "Objetivo: control de acceso a la red: la protección de los servicios de red. Se debe controlar el acceso a los servicios de red tanto internos como externos. Esto es necesario para garantizar que los usuarios que tengan acceso a las redes y a los servicios de red no comprometan la seguridad de estos servicios, garantizando: a) interfaces adecuadas entre la red de la organización y las redes de otras organizaciones, o redes públicas; b) mecanismos de autenticación apropiados para usuarios y equipamiento; c) control de acceso de usuarios a los servicios de información"; 5. "Objetivo: control de acceso al sistema operativo: impedir el acceso no autorizado al computador. Los meca-

nismos de seguridad a nivel del sistema operativo deben ser utilizados para restringir el acceso a los recursos del computador. Estas facilidades deben tener la capacidad de llevar a cabo lo siguiente: a) identificar y verificar la identidad y, si fuera necesario, la terminal o ubicación de cada usuario autorizado; b) registrar los accesos exitosos y fallidos al sistema: c) suministrar medios de autenticación apropiados; si se utiliza un sistema de administración de contraseñas, éste debe asegurar la calidad de las mismas; d) restringir los tiempos de conexión de los usuarios, según corresponda. Se debe disponer de otros métodos de control de acceso, como *"challenge-response"*, si están justificados por el riesgo comercial"; 6. "Objetivo: control de acceso a las aplicaciones. Impedir el acceso no autorizado a la información contenida en los sistemas de información. Las herramientas de seguridad deben ser utilizadas para limitar el acceso dentro de los sistemas de aplicación. El acceso lógico al software y a la información debe estar limitado a los usuarios autorizados. Los sistemas de aplicación deben: a) controlar el acceso de usuarios a la información y a las funciones de los sistemas de aplicación, de acuerdo con la política de control de accesos definida por la organización; b) brindar protección contra el acceso no autorizado de utilitarios y software del sistema operativo que tengan la capacidad de pasar por alto los controles de sistemas o aplicaciones; c) no comprometer la seguridad de otros sistemas con los que se comparten recursos de información; d) tener la capacidad de otorgar acceso a la información únicamente al propietario, a otros individuos autorizados mediante designación formal, o a grupos definidos de usuarios"; 7. "Objetivo: monitoreo del acceso y uso de los sistemas: detectar actividades no autorizadas. Los sistemas deben ser monitoreados para detectar desviaciones respecto de la política de control de accesos y registrar eventos para suministrar evidencia en caso de producirse incidentes relativos a la seguridad. El monitoreo de los sistemas permite comprobar la eficacia de los controles adoptados y verificar la conformidad con el modelo de política de acceso"; 8. "Objetivo: computación móvil y trabajo remoto. Garantizar la seguridad de la información cuando se utiliza computación móvil e instalaciones de trabajo remotas. La protección requerida debe ser proporcional a los riesgos que originan estas formas específicas de trabajo. Cuando se utiliza computación móvil deben tenerse en cuenta los riesgos que implica trabajar en un ambiente sin protección y se debe implementar la protección

adecuada. En el caso del trabajo remoto la organización debe implementar la protección en el sitio de trabajo remoto (*teleworking site*) y garantizar que se tomen las medidas adecuadas para este tipo de trabajo".

Requerimientos de negocio para el control de accesos (Business Requirement for Access Control).

* Política de control de accesos (*Access Control Policy*)

- Requerimientos políticos y de negocios (*Policy and Business Requirements*)

Se deben definir y documentar los requerimientos del negocio para el control de accesos, para cada usuario o grupo de usuarios, en una declaración de política, que contemple: a) requerimientos de seguridad; b) identificación de la información relacionada con las aplicaciones; c) políticas de divulgación y autorización de la información; d) coherencia entre las políticas y de clasificación de información; e) legislación aplicable y obligaciones contractuales; f) perfiles de acceso de usuarios; g) administración de derechos de acceso.

- Reglas de control de accesos (*Access Control Rules*)

En la especificación de las reglas de control de acceso debe considerarse: a) diferenciar entre reglas que siempre deben imponerse y reglas condicionales; b) generalmente todo debe estar prohibido, a menos que se permita expresamente; c) cambios en los rótulos de la información; d) cambios en los permisos de usuario; e) reglas para la aprobación del administrador u otros.

Administración de accesos de usuarios (User Access Management).

* Registración de usuarios (*User Registration*)

Debe haber un procedimiento formal de registro y borrado de registro de usuarios para permitir acceso a todos los sistemas y servicios de información multiusuario, el que tiene que ser controlado por medio de un proceso formal de registración de usuarios.

* Administración de privilegios (*Privilege Management*)

Se debe limitar y controlar la asignación y uso de privilegios, que permita

que el usuario pase por alto los controles de sistemas o aplicaciones, pues su uso inadecuado es el más importante factor que contribuye a las falla de los sistemas.

* Administración de contraseñas de usuario (*User Password Management*)

Las palabras de paso o contraseñas representan un medio común de validación de la identidad de un usuario para acceder a un sistema o servicio de información, por lo que deben controlarse a través de una administración formal.

* Revisión de derechos de acceso de usuario (*Review of User Access Rights*)

La gerencia debe concretar un proceso formal, a efectos de revisar a intervalos regulares, los derechos de acceso de los usuarios y mantener un control del acceso a los datos y servicios de información.

Responsabilidades del usuario (User Responsibilities).

* Uso de contraseñas (*Password Use*)

Los usuarios deben seguir buenas prácticas de seguridad en la selección y uso de contraseñas: a) mantenerlas en secreto; b) evitar un registro en papel; c) cambiar las contraseñas; d) seleccionar contraseñas de calidad; e) no incluirlas en los procesos automatizados de inicio de sesión; f) no compartir las contraseñas individuales de usuario.

* Equipos desatendidos en áreas de usuarios (*Unattended User Equipment*)

Los usuarios deben garantizar que los equipos no atendidos sean protegidos apropiadamente: a) concluir las sesiones activas al finalizar las tareas; b) realizar el procedimiento de salida de los procesadores centrales cuando finaliza la sesión; c) proteger las computadoras o terminales contra usos no autorizados.

Control de acceso a la red (Network Access Control).

* Política de utilización de los servicios de red (*Policy on Use of Network Services*)

Los usuarios solamente deben contar con acceso directo a los servicios para lo que han sido expresamente autorizados, puesto que las conexiones no seguras a los servicios de red pueden afectar a toda la empresa.

* Camino forzoso (*Enforced Path*)

Las redes están diseñadas para posibilitar el máximo alcance de distribución de recursos y flexibilidad, pudiendo resultar necesario controlar el camino desde la terminal del usuario hasta el servicio informático, ya que esas características pueden ofrecer oportunidades para el acceso no autorizado a las aplicaciones de negocios, o para el uso no autorizado de los servicios de información.

* Autenticación de usuarios para conexiones externas (*User Authentication for External Connections*)

Las conexiones externas tienen un gran potencial para los accesos no autorizados a la información del ente, por lo que el acceso de usuarios remotos debe estar condicionado a la autenticación.

* Autenticación de nodos (*Node Authentication*)

Considerando que una herramienta de conexión automática a una computadora remota puede posibilitar un medio para lograr acceso no autorizado a una aplicación de la organización, las conexiones a sistemas informativos remotos deben ser autenticadas.

* Protección de los puertos de diagnóstico remoto (*Remote Diagnostic Port Protection*)

Muchas computadoras y sistemas de comunicación son instalados con una herramienta de diagnóstico remoto por discado, para uso de los ingenieros de mantenimiento, por lo que el acceso a los puertos de diagnóstico debe ser controlado de forma segura, para evitar un medio de acceso no autorizado.

* Subdivisión de redes (*Segregation in Networks*)

Las extensiones de redes pueden incrementar el riesgo de acceso no autorizado a sistemas de información ya existentes que utilizan la red, algunos de los cuales pueden requerir la protección debido a su sensibilidad o criticidad,

por lo que se deben considerar controles dentro de dicha red, a fin de segregar grupos de servicios de información, usuarios y sistemas de información.

* Control de conexión a la red (*Network Connection Control*)

Las necesidades de la política de control de accesos para redes compartidas, especialmente para las que se extienden más allá de los límites de la organización, pueden requerir la introducción de controles para limitar la capacidad de conexión de los usuarios, que pueden implementarse para filtrar el tráfico por medio de reglas previamente definidas.

* Control de ruteo de red (*Network Routing Control*)

Del mismo modo, las redes compartidas pueden precisar la incorporación de controles de ruteo para asegurar que las conexiones informáticas y los flujos de información no salten la política de control de acceso de las aplicaciones comerciales.

* Seguridad de los servicios de red (*Security of Network Services*)

Las organizaciones que utilizan servicios de red, privados o públicos, deben garantizar que se provea de una descripción de los atributos de seguridad de los mismos.

Control de acceso al sistema operativo (Operating System Access Control).

* Identificación automática de terminales (*Automatic Terminal Identification*)

La identificación automática de terminales es una técnica que se emplea si resulta importante que la sesión solamente pueda iniciarse desde una terminal información o una ubicación determinada, debiéndose tener en centa para autenticar conexiones a ubicaciones especificas y a equipamiento portátil.

* Procedimientos de conexión de terminales (*Terminal Log-On Procedures*)

El acceso a los servicios de información debe ser posible por medio de un proceso de conexión seguro, diseñado para reducir la oportunidad de acceso no autorizado.

* Identificación y autenticación de los usuarios (*User Identification and Authentication*)

Todos los usuarios deben tener un identificador único, sólo para su uso personal exclusivo, de forma que las actividades puedan seguirse con posterioridad hasta alcanzar al individuo responsable.

* Sistema de administración de contraseñas (*Password Management System*)

Los sistemas de adminsitración de contraseñas deben representar una herramienta efectiva e interactiva, puesto que las contraseñas constituyen uno de los principales medios de validación de la autoridad de un usuario para acceder a un servicio informático.

* Uso de utilitarios de sistema (*Use of System Utilities*)

Es primordial que el uso de los programas utilitarios de las instalaciones informáticas, sea limitado y cuidadosamente controlado.

* Alarmas silenciosas para la protección de usuarios (*Duress Alarm to Safeguard Users*)

En base a la evaluación de riesgos, debe considerarse la provisión de alarmas silenciosas para los usuarios que podrían ser pasibles de coerción, definiéndose responsabilidades y procedimientos para su activación.

* Desconexión de terminales por tiempo muerto (*Terminal Time-Out*)

Las terminales inactivas en ubicaciones de alto riesgo o que sirven a sistemas de alto riesgo, deben apagarse luego de un periodo definido de inactividad, para evitar el acceso de personas no autorizadas.

* Limitación del horario de conexión (*Limitation of Connection Time*)

Las restricciones al horario de conexión deben proporcionar seguridad adicional a las aplicaciones de alto riesgo.

Control de acceso a las aplicaciones (Application Access Control).

* Restricción del acceso a la información (*Information Access Restriction*)

Los usuarios de sistemas de aplicación deben tener acceso a la información y a las funciones, conforme con una política de control de acceso definida.

Aislamiento de sistemas sensibles (*Sensitive System Insolation*)

Los sistemas sensibles podrían necesitar un ambiente informático aislado, considerando las pérdidas potenciales y el requerimiento de tratamiento especial.

Monitoreo del acceso y uso de los sistemas (Monitoring System Access And Use).

* Registro de eventos (*Event Logging*)

Deben producirse registros de auditoría que tengan excepciones y otros eventos vinculados con la seguridad, manteniéndose durante un período definido para acceder en investigaciones futuras y en el monitoreo del control de acceso, y que contengan: a) identificación de acceso de usuario; b) fecha y hora de inicio y terminación; c) identidad o ubicación de la terminal; d) registros de intentos exitosos y fallidos de acceso al sistema; e) registros de intentos exitosos y fallidos de acceso a datos y otros recursos.

* Monitoreo del uso de los sistemas (*Monitoring System Use*)

- Procedimientos y áreas de riego (*Procedures and Areas of Risk*)

Se deben establecer procedimientos para monitorear el uso de las instalaciones de procesamiento de la información, a fin de garantizar que los usuarios solamente estén desempeñando actividades que hayan sido autorizadas en forma expresa.

- Factores de riesgo (*Risk Factors*)

Se debe revisar en forma periódica el resultado de las actividades de monitoreo, dependiendo la frecuencia de los riesgos involucrados y de los factores de riesgo: a) criticidad de los procesos de aplicaciones; b) valor, sensibilidad o criticidad de la información; c) experiencia acumulada en materia de infiltración y uso inadecuado del sistema; y d) alcance de la interconexión del sistema.

- Registro y revisión de eventos (*Logging and Reviewing Events*)

Una revisión de los registros representa la comprensión de las amenazas que enfrenta el sistema y las formas que surgen, pudiendo existir eventos que requieran investigación adicional de producirse incidentes en materia de seguridad.

* Sincronización de relojes (*Clock Synchronization*)

La adecuada sincronización de los relojes de las computadoras resulta importante para asegurar la exactitud de los registros de auditoria, que pueden requerirse para investigaciones o como evidencia en casos legales o disciplinarios.

Computación móvil y trabajo remoto (Mobile Computing And Teleworking).

* Computación móvil (*Mobile Computing*)

Cuando se emplean dispositivos informáticos móviles (notebooks, palmtops, laptops, teléfonos móviles), debe tenerse especial atención en garantizar que no se comprometa la información de la organización, adoptando una política formal que considere los riesgos involucrados.

* Trabajo remoto (*Teleworking*)

Considerando que el trabajo remoto utiliza tecnología de comunicaciones para posibilitar que el personal trabaje en forma remota desde un lugar fuera de la organización, se debe implementar la protección apropiada del sitio de trabajo remoto contra: robo de equipamiento e información; divulgación no autorizada de información; acceso remoto no autorizado a los sistemas internos de la organización; uso inadecuado de los dispositivos e instalaciones.

2.8. Desarrollo y mantenimiento de sistemas (*Systems Development and Maintenance*).

Se recuerda que en todo trabajo de Tecnología de la Información se debe instaurar y mantener la seguridad mediante el uso de controles en todas las etapas del proceso; destacándose los requerimientos de seguridad de los sistemas de información, en los sistemas de aplicación, los controles criptográficos, la seguridad de los archivos del sistema, y también en los procesos de desarrollo y soporte: 1. "Objetivo: requerimientos de seguridad de los sistemas: asegurar

que la seguridad es incorporada a los sistemas de información. Esto incluirá infraestructura, aplicaciones comerciales y aplicaciones desarrolladas por el usuario. El diseño e implementación de los procesos comerciales que apoyen la aplicación o servicio pueden ser cruciales para la seguridad. Los requerimientos de seguridad deben ser identificados y aprobados antes del desarrollo de los sistemas de información. Todos los requerimientos de seguridad, incluyendo la necesidad de planes de reanudación, deben ser identificados en la fase de requerimientos de un proyecto y justificados, aprobados y documentados como un parte de la totalidad del caso de negocios de un sistema de información"; 2. "Objetivo: seguridad de los sistemas de aplicación: prevenir la pérdida, modificaciones o uso inadecuado de los datos del usuario en los sistemas de aplicación. Se deben diseñar en los sistemas de aplicación, incluyendo las aplicaciones realizadas por el usuario, controles apropiados y pistas de auditoría o registros de actividad. Esto debe incluir la validación de datos de entrada, procesamiento interno y salidas de datos"; 3. "Objetivo: controles criptográficos: proteger la confidencialidad, autenticidad o integridad de la información. Deben utilizarse sistemas y técnicas criptográficas para la protección de la información que se considera en estado de riesgo y para la cual otros controles no suministran una adecuada protección"; 4. "Objetivo: seguridad de los archivos del sistema: garantizar que los proyectos y actividades de soporte de Tecnología de la Información se lleven a cabo de manera segura. Se debe controlar el acceso a los archivos del sistema. El mantenimiento de la integridad del sistema debe ser responsabilidad de la función usuaria o grupo de desarrollo a quien pertenezca el software o sistema de aplicación"; 5. "Objetivo: seguridad de los procesos de desarrollo y soporte: mantener la seguridad del software y la información del sistema de aplicación. Se deben controlar estrictamente los entornos de los proyectos y el soporte de los mismos. Los gerentes responsables de los sistemas de aplicación también deben ser responsables de la seguridad del ambiente del proyecto y del soporte. Los gerentes deben garantizar que todos los cambios propuestos para el sistema sean revisados, a fin de comprobar que los mismos no comprometen la seguridad del sistema o del ambiente operativo".

Requerimientos de seguridad de los sistemas (Security Requirements Of Systems).

* Análisis y especificaciones de los requerimientos de seguridad (*Security Requirements Analysis and Specification*)

Las comunicaciones de necesidades comerciales para nuevos sistemas o mejoras a los sistemas existentes deben especificar las necesidades de controles, considerando los controles automáticos a incorporar al sistema y la necesidad de controles manuales de apoyo; siendo el marco para analizar los requerimientos de seguridad e identificar los controles que los satisfagan, la evaluación y la administración del riesgo. Se destaca que los controles introducidos en la etapa de diseño son mucho más económicos de implementar y mantener que aquellos incluidos durante o después de la implementación.

Seguridad de los sistemas de aplicación (Security in Application Systems).

* Validación de datos de entrada (*Input Data Validation*)

Los datos de entrada en sistemas de aplicación deben ser validados para asegurar que son correctos y apropiados, y los controles deben ser aplicados a las entradas de transacciones del negocio, datos permanentes y tablas de parámetros.

* Controles de procesamiento interno (*Control of Internal Processing*)
- Áreas de riesgo (*Areas of Risk*)

Los datos que han sido ingresados adecuadamente pueden viciarse al procesar errores o a través de actos deliberados, y los controles de validación deben ser introducidos a los sistemas para detectar tal problema.

- Controles y verificaciones (*Checks and Controls*)

Los controles que se requieren dependerán de la naturaleza de la aplicación y del impacto de probables alteraciones de los datos del negocio, pudiéndose incorporar: a) controles de sesión o de lote; b) controles de balance; c) validación de datos generados por el sistema; d) verificaciones de integridad de datos o software; e) totales de control de registros y archivos; f) verificaciones de

ejecución de los programas de aplicación; g) otras comprobaciones para garantizar ejecución de programas.

- Autenticación de mensajes (*Message Authentication*)

La legitimación de mensajes es una técnica empleada para detectar cambios no autorizados en el contenido de un mensaje enviado electrónicamente, o para descubrir alteraciones en el mismo, pudiéndose implementar un dispositivo físico de autenticación de mensajes o un algoritmo de software.

- Validación de los datos de salida (*Output Data Validation*)

La salida de datos de un sistema de aplicación debe ser conformada para asegurar que el procesamiento de la información almacenada sea correcto y apropiado a las circunstancias, construyéndose normalmente los sistemas suponiendo que si se ha llevado a término una validación, verificación y prueba adecuada, la salida será siempre correcta, aunque ello no siempre se cumple. Las comprobaciones de salidas pueden ser: a) revisiones de la razonabilidad; b) control de conciliación de cuentas; c) provisión de información suficiente para controles posteriores; d) procedimientos para responder a las pruebas de validación; e) definición de las responsabilidades del personal relacionado en el proceso de salida de datos.

Controles criptográficos (Cryptographic Controls)

* Política de utilización de controles criptográficos (*Policy on the Use of Cryptographic Controls*)

Una empresa debe desarrollar una política adecuada sobre el uso de controles criptográficos para la protección de su información, considerando: a) el enfoque gerencial; b) el enfoque con relación a la administración de claves; c) funciones y responsabilidades; d) determinación del nivel apropado de protección; e) normas para la implementación.

* Cifrado (*Encryption*)

El cifrado es una técnica criptográfica que puede usarse para proteger la confidencialidad de la información sensible o crítica. Mediante una evaluación

de riesgos debe identificarse el nivel requerido de protección, tomando en consideración el tipo y la calidad del algoritmo de cifrado y la longitud de las claves a utilizar.

* Firma digital (*Digital Signatures*)

Las firmas digitales brindan un medio de protección de la autenticidad e integridad de los documentos electrónicos (firmas de pagos, transferencias de fondos, contratos y convenios electrónicos) y se deben tomar los recaudos para proteger la confidencialidad de la clave privada (creación de una firma) y salvaguardar la integridad de la clave pública (verificación).

* Servicios de no repudio (*Non-Repudiation Services*)

Los servicios de no repudio, que están basados en el uso de técnicas de encriptación y firma digital, deben utilizarse cuando es preciso solucionar disputas acerca de la ocurrencia o no acontecimiento de un evento o acción, pudiendo ayudar a sentar evidencia.

* Administración de claves (*Key Management*)

- Protección de claves criptográficas (*Protection of Cryptographic Keys*)

La administración de claves criptográficas es fundamental para la utilización efectiva de las técnicas criptográficas, debiéndose implementar un sistema de administración para respaldar el uso por la organización de los tipos de técnicas: a) técnicas de clave secreta, b) técnicas de clave pública.

- Normas, procedimientos y métodos (*Standards, Procedures and Methods*)

Un sistema de administración de claves debe estar sustentado en un conjunto consensuado de normas, procedimientos y métodos seguros.

Seguridad de los archivos del sistema (Security of System Files).

* Control del software operativo (*Control of Operational Software*)

Debe proveerse de control para la implementación de software en los sistemas en operaciones considerando diversos controles.

* Protección de los datos de prueba del sistema (*Protection of System Test Data*)

Los datos de prueba deben ser protegidos y controlados. Cuando los datos operativos se utilizan con fines de prueba deben aplicarse controles específicos.

* Control de acceso a las bibliotecas de programa fuente (*Access Control to Program Source Library*)

Se debe mantener un control preciso del acceso a las bibliotecas de software fuente, a fin de reducir la probabilidad de la alteración de programas de computadora.

Seguridad de los procesos de desarrollo y soporte (Security in Development and Support Processes).

* Procedimientos de control de cambios (*Change Control Procedures*)

Debe haber un control estricto de la implementación de los cambios, incluyendo el software de aplicaciones, con el fin de minimizar la alteración de los sistemas de información, imponiéndose el cumplimiento de los procedimientos formales de control de los cambios.

* Revisión técnica de los cambios en el sistema operativo (*Technical Review of Operating System Changes*)

Cuando se realizan los cambios en el sistema operativo, los sistemas de aplicación deben ser revisados y probados para garantizar que no haya un impacto negativo en las operaciones o en la seguridad.

* Restricción del cambio en los paquetes de software (*Restrictions on Changes to Software Packages*)

Los paquetes de software de proveedores deben ser utilizados sin modificación, al menos que se considere esencial, pero teniendo en cuenta: a) el riesgo de comprometer los procesos de integridad y controles incorporados; b) la obtención del consentimiento del proveedor; c) la posibilidad de obtener del proveedor los cambios requeridos; d) el impacto si corresponde que la organización se haga responsable del mantenimiento futuro del programa.

* Canales ocultos y código troyano (*Covert Channels and Trojan Code*)

Los canales ocultos pueden activarse modificando un parámetro mediante elementos de un sistema informático, o incorporando información a un flujo de datos) y el código troyano está diseñado para afectar un sistema en forma no autorizada y difícilmente advertida, por lo que deben considerarse puntos para hacerles frente.

* Desarrollo externo de software (*Outsourced Software Development*)

Al tercerizarse el desarrollo de software, deben considerarse: a) acuerdos de licencias, propiedad de códigos y derechos de propiedad intelectual; b) certificación de la calidad y precisión del trabajo; c) acuerdos de custodia por quiebra de la tercera parte; d) derechos de acceso a una auditoría de la calidad y precisión del trabajo; e) requerimientos contractuales; f) realización de pruebas previas a la instalación.

2.9. Administración de la continuidad de los negocios (*Business Continuity Management*).

Se determina estar preparado para contrarrestar las suspensiones o interrupciones en las actividades de la organización y para proteger sus procesos importantes en caso de fracasos graves o catástrofes: "Objetivo: aspectos de la administración de la continuidad de los negocios: contrarrestar las interrupciones de las actividades comerciales y proteger los procesos críticos de los negocios de los efectos de fallas significativas o desastres. Se debe implementar un proceso de administración de la continuidad de los negocios para reducir la discontinuidad ocasionada por desastres y fallas de seguridad (que pueden ser el resultado de, por ejemplo, desastres naturales, accidentes, fallas en el equipamiento, y acciones deliberadas) a un nivel aceptable mediante una combinación de controles preventivos y de recuperación. Se deben analizar las consecuencias de desastres, fallas de seguridad e interrupciones del servicio. Se deben desarrollar e implementar planes de contingencia para garantizar que los procesos de negocios puedan restablecerse dentro de los plazos requeridos. Dichos planes deben mantenerse en vigencia y transformarse en una parte integral del resto de los procesos de administración y gestión. La administración

de la continuidad de los negocios debe incluir controles destinados a identificar y reducir riesgos, atenuar las consecuencias de los incidentes perjudiciales y asegurar la reanudación oportuna de las operaciones indispensables".

Aspectos de la administración de la continuidad de los negocios (Aspects of Business Continuity Management).

* Proceso de administración de la continuidad de los negocios (*Business Continuity Management Process*)

Se debe implementar un proceso de control para el desarrollo y mantenimiento de la continuidad del negocio que considere aspectos clave.

* Continuidad del negocio y análisis del impacto (*Business Continuity and Impact Analysis*)

La continuidad de los negocios se debe iniciar con la identificación de los eventos que pueden provocar interrupciones en los procesos de negocios (fallas de equipamiento, inundación e incendio, etc.) y luego debe hacerse una evaluación de riesgos para determinar el impacto de dichas interrupciones, para desarrollar un plan estratégico que determine un enfoque global.

* Elaboración e implementación de planes de continuidad de los negocios (*Writing and Implementing Continuity Plans*)

Los planes deben ser desarrollados e implantados para mantener o restablecer las operaciones de los negocios en los tiempos requeridos una vez producida una interrupción o falla en los procesos críticos de los negocios.

* Marco conceptual para la planificación de la continuidad de los negocios (*Business Continuity Planning Framework*)

Debe mantenerse un marco determinado para los planes de continuidad de los negocios, con el objetivo de asegurar su uniformidad e identificar prioridades de prueba y mantenimiento.

* Prueba, mantenimiento y reevaluación de los planes de continuidad de los negocios (*Testing, Maintaining and Re-assessing Business Continuity Plans*)

- Pruebas de los planes (*Testing the Plans*)

Los planes de continuidad de los negocios pueden fallar durante el curso de las pruebas, debido a supuestos incorrectos, negligencias o cambios en el equipamiento o el personal, por lo que deben ser probados periódicamente para garantizar que se hallen actualizados y son efectivos.

- Mantenimiento y reevaluación del plan (*Maintaining and Re-assessing the Plans*)

Los planes mencionados deben mantenerse mediante revisiones y actualizaciones periódicas para asegurar su eficacia permanente.

2.10. Cumplimiento (***Compliance***).

Se imparten instrucciones a las organizaciones para que verifiquen si el cumplimiento con la norma concuerda con otros requisitos jurídicos, legales o contractuales aplicables. También, se requiere una revisión de las políticas de seguridad, destacándose las consideraciones técnicas con respecto al proceso de auditoría de sistemas: 1. "Objetivo: cumplimiento de requisitos legales: impedir infracciones y violaciones de leyes; de las obligaciones establecidas por leyes, estatutos, normas, reglamentos o contratos; y de los requisitos de seguridad. El diseño, operación, uso y administración de los sistemas de información pueden estar sujetos a requisitos de seguridad legal, normativa y contractual. Se debe procurar asesoramiento sobre requisitos legales específicos por parte de los asesores jurídicos de la organización, o de abogados convenientemente calificados. Los requisitos legales varían según el país y en relación con la información que se genera en un país y se transmite a otro (por ejemplo, flujo de datos a través de fronteras"; 2. "Objetivo: revisiones de la política de seguridad y la compatibilidad técnica: garantizar la compatibilidad de los sistemas con las políticas y normas de seguridad de la organización. La seguridad de los sistemas de información debe revisarse periódicamente. Dichas revisiones deben llevarse a cabo con referencia a las políticas de seguridad pertinentes y las plataformas técnicas y los sistemas de información deben ser auditados para verificar su compatibilidad con los estándares (normas) de implementación de seguridad"; 3. "Objetivo: consideraciones de auditoría de

sistemas: optimizar la eficacia del proceso de auditoría de sistemas y minimizar los problemas que pudiera ocasionar el mismo, o los obstáculos que pudieran afectarlo. Deben existir controles que protejan los sistemas de operaciones y las herramientas de auditoría en el transcurso de las auditorías de sistemas. Asimismo, se requiere una protección adecuada para salvaguardar la integridad y evitar el uso inadecuado de las herramientas de auditoría".

Cumplimiento de requisitos legales (Compliance with Legal Requirements).

* Identificación de la legislación aplicable (*Identification of Applicable Legislation*)

Deben definirse y documentarse todos los requerimientos legales, normativos y contractuales pertinentes para cada sistema de información, al igual que los controles específicos y las responsabilidades individuales para cumplir con los mismos.

* Derechos de propiedad intelectual (DPI) (*Intellectual Property Rights - IPR*)
- Derecho de propiedad intelectual (*Copyright*)

Se deben implementar procedimientos apropiados para garantizar el cumplimiento de las restricciones legales al uso del material respecto del que puedan existir derechos de propiedad intelectual, derechos de diseño o marcas registradas.

- Derecho de propiedad intelectual del software (*Software Copyright*)

Los productos de software que sean propiedad de una empresa se suministran normalmente bajo un acuerdo de licencia que limita el uso de los productos a máquinas específicas y puede restringir la copia a la creación de copias de resguardo solamente, por lo que deben considerarse los controles pertinentes.

- Protección de los registros de la organización (*Safeguarding of Organizational Records*)

Los registros importantes de la empresa deben protegerse contra pérdida, destrucción y falsificación, y algunos registros pueden requerir una retención

segura para cumplir con requerimientos legales o normativos, y para respaldar las actividades esenciales del negocio. Deben ser clasificados en diferentes tipos: registros contables, registros de base de datos, logs de transacciones, logs de auditoría y procedimientos operativos; cada uno de ellos detallando los períodos de retención y el tipo de medios de almacenamiento (papel, microfichas, medios magnéticos u ópticos).

- Protección de los datos y privacidad de la información personal (*Data Protection and Privacy of Personal Information*)

Diversos países han incorporado leyes que establecen controles sobre el procesamiento y transmisión de datos personales, y pueden imponer responsabilidades a las personas que recopilan, procesan y divulgan información personal, y pueden limitar la capacidad de transferir dichos datos a otros territorios. El cumplimiento de la legislación sobre protección de datos precisa de una estructura y un control de gestión adecuados.

- Prevención del uso inadecuado de los recursos de procesamiento de la información (*Prevention of Misure of Information Processing Facilities*)

Los recursos de procesamiento de información de una empresa se proporcionan con fines de negocios y la gerencia debe autorizar el uso que se da a los mismos; su utilización con propósitos no autorizados puede constituir un delito criminal por lo que es imprescindible que todos los usuarios estén enterados del alcance preciso del acceso permitido.

- Regulación de controles para el uso de criptografía (*Regulation of Cryptographic Controls*)

Ciertos países han implementado acuerdos, leyes, normas y otros instrumentos para controlar el acceso a los controles criptográficos o el uso de los mismos, debiéndose procurar un asesoramiento jurídico para garantizar el cumplimiento de las normas nacionales.

* Recolección de evidencia (*Collection of Evidence*)

- Reglas para la recolección de evidencia (*Rules for Evidence*)

Es preciso contar con una evidencia apropiada para soportar una acción contra una persona u organización.

- Validez de la evidencia (*Admissibility of Evidence*)

Las organizaciones deben garantizar que sus sistemas de información cumplan con las normas o códigos de práctica relacionados con la producción de evidencia válida.

- Calidad y totalidad de la evidencia (*Quality and Completeness of Evidence*)

La calidad y totalidad de la evidencia se logra con una sólida pista de la misma, ya sea para documentos en papel como para información en medios informáticos.

Revisiones de la política de seguridad y la compatibilidad técnica (Reviews of Security Policy and Technical Compliance).

* Cumplimiento de la política de seguridad (*Compliance with Security Police*)

La gerencia debe asegurar que se sigan correctamente todos los procedimientos de seguridad dentro del área de su responsabilidad, y considerar la implementación de una revisión periódica de todas las áreas de la organización (sistemas de información, proveedores de sistemas, propietarios de información y recursos de información, usuarios, gerentes) para garantizar el cumplimiento de las políticas y normas de seguridad.

* Verificación de la compatibilidad técnica (*Technical Compliance Checking*)

Debe verificarse periódicamente la compatibilidad de los sistemas de información con las normas de implementación de seguridad, comprendiendo la revisión de los sistemas operacionales, a fin de asegurar que los controles de hardware y software hayan sido correctamente implantados.

Consideraciones de auditoría de sistemas (Systems Audit Considerations).

* Controles de auditoría de sistemas (*System Audit Controls*)

Los requerimientos y actividades de auditoría que representan verificaciones de los sistemas operacionales deben ser planificados y acordados, a efectos de reducir el riesgo de discontinuidad de los procesos de negocio: a) los pedidos de auditoría deben ser consensuados con la gerencia respectiva; b)

deben acordarse y controlarse el alcance de las verificaciones; c) las revisiones deben estar limitadas a un acceso solamente de lectura del software de datos; d) pueden permitirse accesos para copias aisladas de archivos del sistema; e) deben identificarse y poner a disposición los recursos de tecnología de la información para concretar las verificaciones; f) corresponde individualizar y convenir los requerimientos de procesamiento especial; g) los accesos deben ser monitoreados y registrados para generar pistas de referencia; h) deben documentarse todos los procedimientos, solicitudes y responsabilidades.

• Protección de las herramientas de auditoría de sistemas (*Protection of System Audit Tools*)

Debe protegerse el acceso a las herramientas de auditoría de sistemas (archivos de datos o software) con el objetivo de evitar su uso incorrecto, las que deben estar separadas de los sistemas operacionales y de desarrollo, no resultando conveniente almacenarse en bibliotecas de cintas o en áreas de usuarios, salvo que se les otorgue un nivel apropiado de protección adicional.

3. Algunos Términos y Definiciones de la Norma

- ***Administración de riesgos***: proceso de identificación, control y minimización o eliminación, a un costo aceptable, de los riesgos de seguridad que podrían afectar a los sistemas de información.
- ***Bombas lógicas***: programas que se activan al producirse un acontecimiento determinado; la condición suele ser una fecha, una combinación de teclas, o un estilo técnico. Si no se produce la condición permanece oculto al usuario.
- ***Confidencialidad***: garantía de que acceden a la información, sólo aquellas personas autorizadas a hacerlo.
- ***Disponibilidad***: garantía de que los usuarios autorizados tienen acceso a la información y a los recursos relacionados con la misma, toda vez que lo requieran.
- ***Evaluación de riesgos***: evaluación de las amenazas, impactos y vulnerabilidades relativas a la información y a las instalaciones de procesamiento de la misma, y a la probabilidad de que ocurran.

- ***Hacking*** (pirateo): acción clandestina o de piratear sistemas informáticos y redes de comunicación.
- ***Integridad***: mantenimiento de la exactitud y totalidad de la información y los métodos de procesamiento.
- ***Logging***: registro de actividades en un archivo informático, de diferentes situaciones; se utiliza normalmente como evidencia de auditoría.
- ***Logs***: registros de situaciones en un sistema informático, tales como actividades de usuarios, control de contraseñas, etc., siendo el resultado de puesta en marcha del *logging*.
- ***Password*** (contraseña): conjunto de caracteres alfanuméricos que permite a un usuario, el acceso a un determinado recurso o la utilización de un servicio dado.
- ***Seguridad de la información***: preservación de la confidencialidad, integridad y disponibilidad de la información.
- ***Software malicioso***: término común que se utiliza al referirse a cualquier programa inesperado o a códigos como virus, troyanos o programas de broma.
- ***Troyanos***: programas maliciosos que, en forma similar al "caballo de Troya", ocultan sus intenciones reales bajo la apariencia de un juego o una animación; permiten el acceso al equipo infectado, borran archivos, introducen virus o comprometen la seguridad del sistema.
- ***Virus***: programas capaces de autorreproducirse copiándose en otro programa al que infectan, todo ello sin conocimiento del usuario, teniendo la misión que le ha encomendado el programador.
- ***World Wide Web*** (web): universo de información accesible a través de Internet, una fuente continua del conocimiento humano
- ***Worms*** (gusanos): programas que tratan de reproducirse a sí mismo, siendo su objetivo colapsar el sistema.

4. Comentarios Finales

La ISO/IEC 17799 es un estándar internacional cuasi pionero para la seguridad de la información, publicado por primera vez como ISO/IEC 17799:2000

por la *International Organization for Standarization* y por la Comisión Electrónica Internacional, con el título de *Information Tecnology - Security Techniques - Code of Practice for Information Security Management* (en castellano, Tecnología de la información. Técnicas de seguridad. Código de práctica para la gestión de la seguridad de la información). El estándar ISO/IEC tiene su origen en el *British Standard* BS 7799-1 que fue publicado por primera vez en 1995.

El estándar ISO/IEC 17799 tiene equivalentes directos en muchos otros países. La traducción y publicación local suele demorar cierto tiempo. Tras un período de revisión y actualización de los contenidos del estándar, se publicó en el año 2005 un documento actualizado, el estándar ISO/IEC 27002/2005. En nuestro país, la norma IRAM/ISO/IEC 17799/2002 fue reemplazada por la norma argentina IRAM-ISO/IEC 27002 del 15 de agosto de 2008.

El contenido del estándar internacional ISO/IEC 27002 tiene el siguiente esquema:

0. Introducción
1. Ámbito de aplicación
2. Términos y definiciones
3. Estructura del estándar (norma)
4. Valoración del riesgo y tratamiento
5. Política de seguridad
6. Organización de la seguridad de la información
7. Gestión de activos
8. Recursos humanos de seguridad
9. Seguridad física y ambiental
10. Comunicaciones y operaciones de gestión
11. Control de acceso
12. Sistemas de información de adquisición, desarrollo y mantenimiento
13. Seguridad de la información de gestión de incidentes
14. Gestión de la continuidad de negocios
15. Cumplimiento

Después de la introducción, alcance, terminología y las secciones de su es-

tructura, la terminología del estándar especifica 39 objetivos de control para proteger la información contra las amenazas a su confidencialidad, integridad y validez.

Nos remitimos a la lectura y estudio actualizado de la norma argentina.[6]

Notas

DYG.124.PP.3.q1

[1:] Casal, Armando M.: "Las buenas prácticas para la gestión de la seguridad de la información" - LL - Enfoques (Contabilidad y Administración) - diciembre/2005

DYG.124.PP.3.q2

[2:] IRAM, Norma Argentina IRAM-ISO/IEC 17799, "Tecnología de la Información. Código de Práctica para la Gestión de la Seguridad de la Información" - 1a. ed. - 30/8/2002

DYG.124.PP.3.q3

[3:] ISO, *International Organization for Standardization, ISO/IEC 17799, "Information Technology. Code of Practice for Information Security Management"* - 1a. ed. - 1/12/2000

DYG.124.PP.3.q4

[4:] IRAM, Norma argentina IRAM 17798, "Tecnología de la Información. Requisitos para los Sistemas de Gestión de Seguridad de la Información" - 1a. ed. - 2004

DYG.124.PP.3.q5

[5:] ISACA, *Information Systems Audit. and Control Association - "Information Security Harmonisation.Classification of Global Guidance"* - 2005

DYG.124.PP.3.q6

[6:] IRAM, norma argentina IRAM-ISO/IEC 27002, "Tecnología de la Información. Técnicas de seguridad. Código de práctica para la gestión de la seguridad de la información - 1a. Ed. - 15/8/2008

ARMANDO M. CASAL: Contador Público (UBA). Licenciado en Administración (UBA). Director de D&G Profesional y Empresaria -ERREPAR.